Cyber Security Considerations for Autonomous Tactical Wheeled Vehicles

Sebastian C Iovannitti

4/1/2016

Submitted to Lawrence Technological University College of Management in partial fulfillment of the degree of Master of Global Leadership and Management

Submitted to Defense Acquisition University in partial fulfillment of the requirement of the Senior Service College Fellowship

Approval Page

Title: Cyber Security Considerations for Autonomous Tactical Wheeled Vehicles

Author: Sebastian C Iovannitti

Organization: Program Executive Office (PEO) Combat Support & Combat Service Support (CS&CSS)

Date of Paper: April 1, 2016

IRB Approval:	Date: November 05, 2015
OPSEC Approval:	Date:
Approval:	Date:
Approval:	Date:
Approval:	Date:

Submission Date to DAU Library:

Submission Date to Acquisition Research Journal:

Table of Contents

Contents

List of Figures

List of Tables

Abstract

This study will assess the ability of PMs to manage cyber security risks on ground vehicles, review current Cyber Security policy and determine if awareness of cyber risks has increased since Boyd's study (Boyd, 2008). Innovations in autonomous vehicle systems in the commercial truck industries will migrate into Army tactical wheeled vehicles as the Army moves increasingly into autonomous tactical vehicles. The study will identify how current military cyber policy impact cyber incidents (Rosenzweig D. I., 2014) (Rosenzweig P. , 2012) Army PMs were surveyed and they perceive an increased risk using a globalized contractor and some lack the resources to implement the cyber policies. The paper recommends to the Army establish an Autonomy Consortium, introduce cyber physical systems to DoDI 8500.01, and prioritize cyber requirements within the PPBE process.

Chapter 1 - Introduction

Background

Recent cyber security breaches of private industry (Snyder B. , 2014) (Dewey, 2013) (Nakashima, 2013) (Mick, 2011) and government (Miklaszewski, 2015) (Office of Personnel Management, n.d.) (Bryan & Gulzelsu, 2014) (Barkoviak, 2009) have increased awareness of the importance of Cyber Security, and its impacts on the nation (James Gosler, 2012). As President Obama stated:

> In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place...But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage…Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant (Office of the Press Secretary, 2015).

The White House added that cybersecurity is a shared responsibility between the private and public sectors:

> The Federal government has the responsibility to protect and defend the country and we do this by taking a whole-of-government approach to countering cyber threats. This means leveraging homeland security, intelligence, law enforcement, and military authorities and capabilities, which respectively provide for domestic preparedness, criminal deterrence and investigation, and our national defense. Yet much of our nation's critical infrastructure and a diverse array of other potential targets are not owned by the Federal government. The Federal government cannot, nor would Americans want it to, provide cybersecurity for every private network. Therefore, the private sector plays a crucial role in our overall national network defense… (The White House;Office of the Press Secretary, 2015)

President Obama, established "The Comprehensive National Cybersecurity Initiative," that established the procedures the Acquisition community should use to manage future of Acquisition programs.

Problem Statement

Many of the commercial automotive (Ackerman, 2015) and technologies companies have initiated (Google, 2015) (Gary Silberg KPMG LLP, p. 14) efforts to introduce new safety features into vehicles such as lane keeping, adaptive cruise control, blind spot detection, and other driver warning related features that improve overall safety. Over the next five to 10 years these features will evolve into autonomous vehicles (Silberg, p. 7). Many of these features , such as drive by wire systems, sensors, automotive communication networks and sensors are finding their way into commercial trucking fleets (Silberg, p. 7), and the Army's Tactical Wheeled Mr. Kevin Fahey recently stated "Times have changed …the commercial sector achieves the breakthrough, and the military adopts and adapts it to meet our requirements." (Fahey, 2015, p. 5). The Army's science and technology efforts are focused on integrating and evaluating these commercial safety technologies to enable the Army's Tactical Wheeled Vehicles to reduce driver fatigue, convoy casualties, and enable the vehicle crew to identify hazards (Theisen, Autonomous Mobility Appliqué System (AMAS), 2011, pp. 5-10) as, Dr. Roger's discusses :

> Autonomous Mobility Appliqué System technology, successfully demonstrated several times this year by TARDEC and Lockheed Martin, can solve these problems by providing our drivers with viable options, up to and including: conducting manned or optionally-manned missions; utilizing a suite of driver-assist features, such as adaptive cruise control, collision-mitigating braking, lane-keeping assist, electronic stability and rollover warnings; or operating in the fully autonomous mode (TARDEC Public Affairs, 2014) .

Ultimately, these capabilities will evolve into fully autonomous tactical wheeled vehicles that will require reduced occupant interaction to manage the vehicle resulting in the trucks' autonomous systems performing much of the decision making (McNally, 2014). These fully autonomous systems will require connectivity to internal sub-systems to enable autonomous or

remote vehicular control, which will require external communications. Remote operation during times of conflict when the autonomous system may not be capable to perform its functions and telemetry for battle space awareness (ARCIC, 2014, p. 2) would require integrated access to the tactical network. The integration of onboard control capabilities and external communications pose a cyber-security risk that must be assessed (U.S. Department of Transportation , 2014) (Atkinson, 2015). As many of the new technologies and systems are developed in the commercial sector and transitioned into the defense market it is critical to understand the global supply chain that developed and produced them to help identify potential vulnerabilities. To help mitigate these risks, it is essential to achieve reciprocity. Reciprocity is a process that enables a receiving organization to accept or reject the security qualifications of a system that will be integrated into their product. Reciprocity will be an essential across the platform information technology (PIT) for integration of the complex systems required. Lastly to achieve reciprocity and execute the DoDI Cybersecurity standards the information system security managers (ISSM) must have the authority, resources and support necessary to mitigate cyber risks.

Purpose of this Study

This study will assess the ability of PMs to manage cyber security risks on ground vehicles, and determine if awareness of these risks has increased since Boyd's study (Boyd, 2008). The study will review current Cyber Security policy and generate a timeline related to the policy creations in comparison to cyber incidents to identify how the policies have impacted the reoccurrence of cyber incidents. As the commercial truck industries innovate in the field of autonomy, these innovations will migrate into the Army autonomous tactical wheeled vehicles, As the hardware and software needed to enable these capabilities is integrated onto Army

autonomous tactical wheeled vehicles, it is crucial that risks, specifically cybersecurity risks be addressed given that much of the commercial technology may be developed using globalized contractors. Moreover, with the recent increases in cyber incidents and the Army moving into autonomous tactical vehicles, the researcher wanted to identify to what degree the existing policy related to platform information technology (PIT) describes the systems in Army PM Systems and does cyber physical systems be a more appropriate term in support of autonomous tactical wheeled vehicles systems.

Research Questions

1. Has awareness of cyber security risks increased since the 2008 study on software, hardware, and supply chain risk? (Boyd, 2008) .
2. Do Army project managers (PM) have the resources to support cyber security requirements related to the Information system security manager (ISSM)?
3. What challenges do Army PMs perceive with reciprocity related to cyber security?
4. What do Army PMs think opportunities are to obtain Reciprocity with other PMs?

Significance of This Research

This research will bring awareness associated with cyber security risks associated with autonomous vehicle technologies. It will help ensure that cyber risks in areas such as intra-vehicle system networks are identified and managed.

The paper will also address cyber risks associated with non-U.S suppliers, which may poise additional risks and management challenges.

Overview of the Research Methodology

This research paper will review the policies, survey Army Acquisition Project Managers (PM)s , review related research subjects on , and the 2008 Boyd paper on the Globalized Military Industry. It will also evaluate DoDI 8500.01 and DoDI 8510.01 have impacted Federal

cyber breaches. This research will be mixed methods, using quantitative data from a survey, and qualitative data from open comments in the survey. The survey was sent to 168 Army program managers.

The objectives of this research are to identify areas that have increased in awareness since the Boyd study, and identify what possible cyber security requirements could be provided for autonomous tactical wheeled vehicles, based on the research currently available and areas of cyber security risk as defense contractors are forced to become globalized as the U.S. Defense budgets continue to decline. Lastly, the study presents a method by which cyber requirements could be evaluated for autonomous tactical wheeled vehicle systems. The Army PMs surveyed identified that risks exist when using a globalized contractor. In many cases the perceived risks have increased since Boyd's study in 2008. The Army PMs provided that while they have an ISSM with the authority and responsibility, 45% responded that the ISSM does not have the support required to perform their duties.

Limitations of the Study

This research will be limited to the policy and guidance areas related to Cyber Security and associated areas and the survey questions associated with the scope of the previous study that Boyd conducted to answer "What are the risks of dealing with a globalized industrial base?, Do current Army PMs recognize these risks and understand how to manage them? What does industry do to train their PMs for this environment?." (Boyd, 2008, p. 5). It will not address the information technology systems, terrestrial or satellite tactical networks. However, this should be considered in future research areas, or reviewed, as much of the initial literature review supports significant coverage of Information Technology systems. Lastly as cyber security is a sensitive subject this study will be limited to publicly available information.

Chapter 2 – Literature Review

This chapter is a literature review of topics that are integral to understand the increasing risks that are present and relate to the risks associated with autonomous tactical wheeled vehicles. Globalization demonstrates a higher overall cyber risk as defense sector given the global competition and consolidation of the defense industry. Also as more breaches in the U.S. Government systems become known the US Government has responded retroactively to emplace policies that have not been effective in decreeing or deterring future breaches.

Research Project Requirements

Chapter 1 introduces the various leadership policies, past cyber breaches, increased autonomous vehicles in the commercial industry, and the Army's desire to explorer and introduce autonomous tactical wheeled vehicles into the future forces. This chapter will address the following:

- Globalization of the Defense Industry
- Defense Industrial Cyber Breaches and Policy Impacts
- Cyber Physical System Research
- Cyber Security Impacts to Autonomous Tactical Wheeled Vehicles

Globalization of the Defense Industry

While there are many definitions of "globalization", the one proposed by the International Monetary Fund is "the growing economic interdependence of countries world-wide through the increasing volume and variety of cross border transactions in goods and services and of international capital flows, and also through the more rapid and widespread diffusion of technology." (International Monetary Fund, 1997).

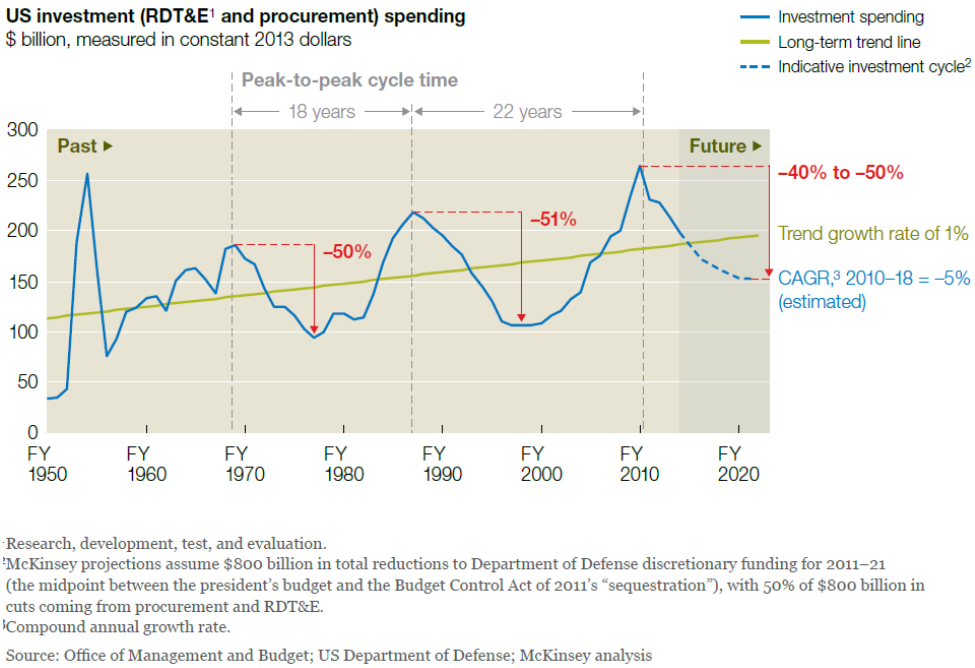
Globalization has blurred the distinction between a domestic and foreign defense company, and policies are not helping either national security or the defense industrial base. The relationship between globalization and technology provides both risks and opportunities, and policies geared

toward preserving a perceived U.S. advantage in technology may prove to be detrimental to both national security and economic competitiveness (Guay, 2007).

Bill Lynn, former Deputy Secretary of Defense from 2009 until 2011, provides that U.S. defense industrial complex has entered a new phase characterized by globalization of supply chains and the lack defense contractors and laboratories to drive technological change. Department of Defense can no longer depend on the American Defense industry to provide it with high-tech components used in advanced weapons systems (McCormack, 2015). "The Pentagon cannot get stuck in a protectionist view of technology… It cannot restrict access to commercial technology since so much of it originates from foreign suppliers. The key point is we need to manage the transition to this [new] industrial base era." (McCormack, 2015)

The Department of Defense is dependent on foreign manufacturers for many of the military's most advanced weapons systems. The industry has little impact on the latest technology developments such as 3D printing, autonomous vehicles and information technology and has shifted from a being an exporter of technology to an importer. Many of the underlying technologies now reside outside of the United States and a lack of visibility at the first or second layer of the supply chain and no visibility beyond that at all. Defense companies that are aggressive in knowing what their supply chain is and they will be able to deliver products that are uncompromised using a more aggressive risk-management approach, since industry owns the supply chain. (McCormack, 2015)

As shown in Figure 1 below, US investments in RDT&E and Procurement spending typically declines approximately 50% post major US military events, and accepting the 50% measured drop, the RDT&E and procurement dollars have yet to reach the a projected low expected in the 2020 timeframe.



[1]Research, development, test, and evaluation.
[2]McKinsey projections assume $800 billion in total reductions to Department of Defense discretionary funding for 2011–21 (the midpoint between the president's budget and the Budget Control Act of 2011's "sequestration"), with 50% of $800 billion in cuts coming from procurement and RDT&E.
[3]Compound annual growth rate.

Source: Office of Management and Budget; US Department of Defense; McKinsey analysis

Figure 1 US investment (RDT&E and Procurement) Spending **(Kevin Dehoff, 2013)**

As the US RDT&E and procurement dollars continue to decline, US defense companies driven by market forces will have to seek replacement income in the global defense and commercial market place which will lead to diffusing the technologies across the globe.

The global redistribution of military technology may have less to do with underfunding in America than with continued Asian economic development. As defense industrial capability develops, defense leaders will face difficult decisions about which military technologies to produce at home and which to buy from an increasingly capable global defense industrial base (Benjamin Braun, 2015, p. 15).

Globalization has provided the U.S. defense industry the change to be more efficient. Like commercial industry has offshored work to save money, the defense industry has done the same. This process is seen thru partnering, acquisitions, mergers, or contractual relationships with foreign owned companies that have an advantage within a host nation's defense sector. This efficiency can

be in the ability to manufacture items or in the knowledge of the working of items such as prohibited materials, which may be different than those in the US, regulatory compliance and agreed in cases thru offsets within Direct Commercial Sales or Foreign Military Sales. This also requires dependence on the foreign owned interest to supply the cyber security measures associated with the US defense company. The work transiting globally includes design, development, and production of both hardware and software, which may be leveraged both outside and within the US Defense markets.

This transition is visible in the expansion of a review of the top 22 department of defense contractors identified by General Services Administration report of "Global Vendor Name", that comprise approximately 45% of the total dollars expended in 2014.

Table 1 2014 Top 22 US DoD companies **(Federal Procurement Data System - Next Generation, 2014, p. DoD Tab)**

Global Vendor Name	Dollars Obligated
LOCKHEED MARTIN CORPORATION	$25,065,461,247.84
THE BOEING COMPANY	$18,005,350,332.68
GENERAL DYNAMICS CORPORATION	$13,630,604,800.84
RAYTHEON COMPANY	$11,816,577,883.63
NORTHROP GRUMMAN CORPORATION	$9,213,821,365.01
UNITED TECHNOLOGIES CORPORATION	$6,117,086,747.69
L-3 COMMUNICATIONS HOLDINGS INC.	$5,288,631,065.98
BAE SYSTEMS PLC	$4,876,213,940.43
HUNTINGTON INGALLS INDUSTRIES INC.	$4,025,292,235.52
HUMANA INC.	$3,527,209,086.24
UNITEDHEALTH GROUP INCORPORATED	$3,203,771,598.01
HEALTH NET INC.	$3,086,459,475.28
SAIC INC.	$2,988,612,860.95
UNITED LAUNCH ALLIANCE L.L.C.	$2,519,158,433.33
BECHTEL GROUP INC.	$2,476,019,275.51
GENERAL ELECTRIC COMPANY	$2,200,317,806.74
BOOZ ALLEN HAMILTON HOLDING CORPORATIO	$2,166,187,575.84
EXELIS INC.	$2,105,471,497.30
BELL BOEING JOINT PROJECT OFFICE	$2,018,971,983.94
HEWLETT-PACKARD COMPANY	$1,766,447,587.13
MCKESSON CORPORATION	$1,663,708,861.81
TOTAL	$127,761,375,661.70

These defense companies identify business risks in their Security and Exchange Commission (SEC) 10K filings. Examples of these risks arise from both the international customer's base, the increasing risk of cyber security disruptions and international agreements requiring use of offsets. Offset are defined as "Compensation practices required as a condition of purchase in either government-to-government or commercial sales of "defense articles" and/or "defense services" as defined by the Arms Export Control Act (22 U.S.C. § 2751, et seq.) and the International Traffic in Arms Regulations (22 C.F.R. §§ 120-130). As seen in the following statements, there exists risks associated with direct commercials sales requiring offsets by US Defense companies.

> "…2014, 20% of our net sales were from international customers…. Offset agreements may require…, technology transfers, local manufacturing support, investments in foreign joint ventures … may require the establishment of a venture with a local company, which must control the venture. Our business could be negatively affected by cyber or other security threats or other disruptions.…seek to minimize the impact of cyber threats…we must rely on the safeguards put in place by these [foreign] entities, which may affect the security of our information. These [foreign] entities have varying levels of cyber security expertise and safeguards and their relationships with government contractors, such as Lockheed Martin, may increase the likelihood that they are targeted by the same cyber threats we face" (Lockheed Martin, pp. 11,13)

> **"Sales and operations outside the U.S. are subject to different risks that may be associated with doing business in foreign countries.** … Our non-U.S. business is subject to …, technology transfers…We may also be required to agree to specific in-country… offsets…and could require us to establish joint ventures with local companies. If we do not satisfy these financial or offset requirements, our future revenues and earnings may be materially adversely affected." (GENERAL DYNAMICS CORPORATION, 2014, p. 14)

> ***"Our international business is subject to geopolitical and economic factors, regulatory requirements and other risks.***
>
> … In 2014, our sales to customers outside the U.S. (including foreign military sales through the U.S. Government) accounted for 29% of our total net sales….Our international sales are also subject to local government laws, regulations, and procurement policies and practices… include[ing] regulations relating to… technology transfer, investments, exchange controls and repatriation of earnings….Our international contracts may include industrial cooperation agreements requiring specific in-country… manufacturing agreements …may require the creation of a joint venture with a local company, which may control the venture… We also are exposed to risks associated with

> using third-party foreign representatives and consultants for international sales and operations, and teaming with international subcontractors, partners and suppliers in connection with international programs." (RAYTHEON COMPANY, 2015, pp. 12-13)
>
> "Our international business exposes us to additional risks. Sales to customers outside the U.S. are an increasingly important component of our strategy. Our international business… contracts may include industrial cooperation agreements requiring specific in-country purchases, investments, manufacturing agreements or other financial obligations, known as offset obligations, and provide for significant penalties if we fail to meet such requirements. The services and products we provide internationally… are…in countries with unstable governments and/or developing legal systems, in areas of military conflict or at military installations. This increases the risk … loss of property or damage to our products." (NORTHRUM GRUMMAN, 2015, pp. 8-9)
>
> "We conduct our business on a global basis, with approximately 61 percent of our 2014 total segment sales derived from international operations…. a condition of sale or award of a contract, …require us to agree to offset arrangements,…penalties in the event we fail to perform in accordance with the offset requirements. In addition, as part of our globalization strategy, we have invested in certain countries, including Argentina, Brazil, China, India, Indonesia, Mexico, Poland, Russia, South Africa and countries in the Middle East, that carry high levels of currency…." (UNITED TECHNOLOGIES CORP, 2015, pp. 12-13)

As reported by the U.S. Department of Commerce Bureau of Industry and Security, March 2015, "Offsets in Defense Trade Nineteenth Study", "During 1993-2010, a total of 61 U.S. firms reported 11,353 offset transactions with 50 countries…[totaling] $56.22 billion…" (U.S. Department of Commerce Bureau of Industry and Security, 2015, p. 4) There has been about a 24% increase in the linear trend of offset agreements as shown in Figure 2. As these offsets increase year over year and companies are looking more and more to foreign markets for their products and services, this creates an increased risk of cyber security across the U.S. DoD given the requirements necessary to meet the offset agreements requiring specific in-country manufacturing, technology transfers and local control of a joint venture.

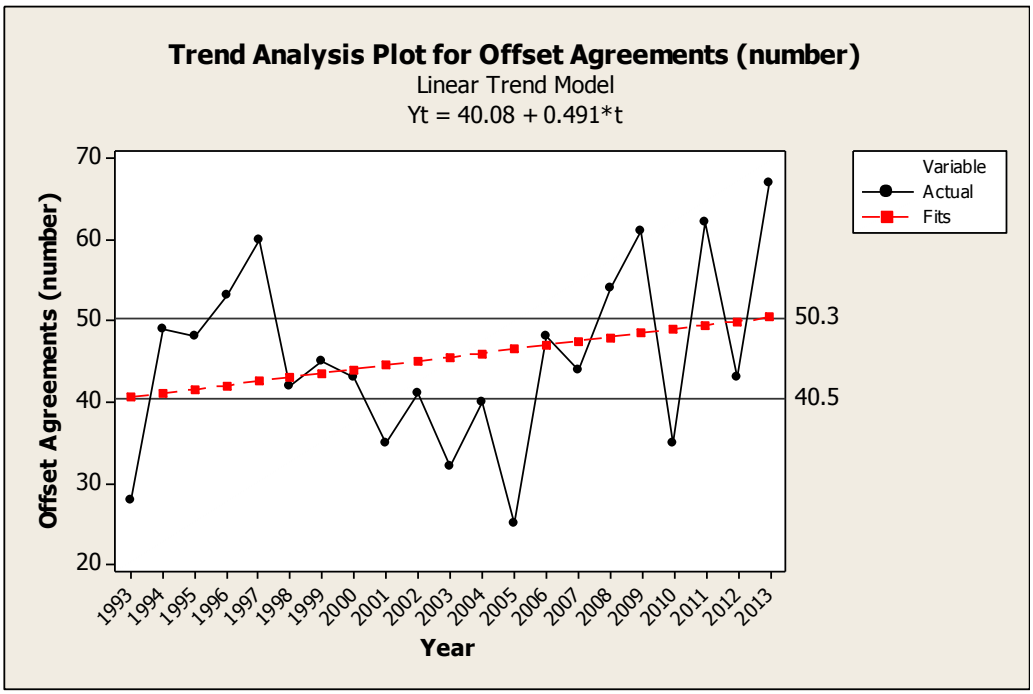


Figure 2 Offset Agreements **(U.S. Department of Commerce Bureau of Industry and Security, 2015)**

Defense Industrial Cyber Breaches and Policy Impacts

Cyber breaches in US. Government systems have increased over the past decade. (Rosenzweig D. I., 2014) (Rosenzweig P. , 2012)

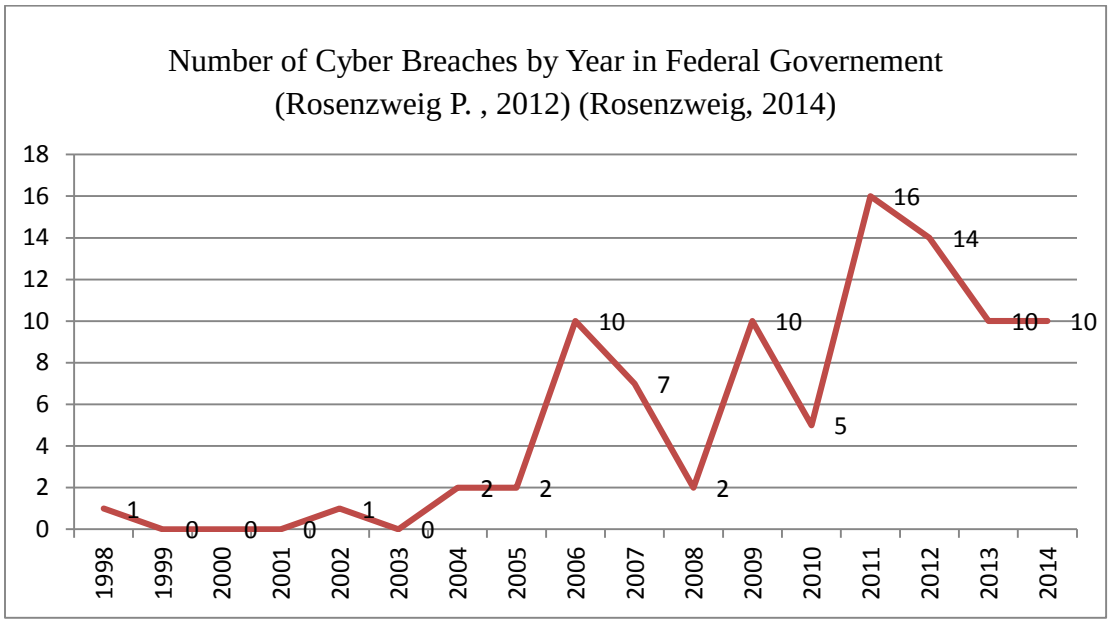


Figure 3 Number of Cyber Breaches by Year in Federal Government (Rosenzweig P. , 2012) (Rosenzweig, 2014)

Figure 4, below, reflects the number of individual references added or introduced into Department of Defense Instruction (DoDI) 8500.01 Policy Appendices titled "Cybersecurity" located on pages 8-13.

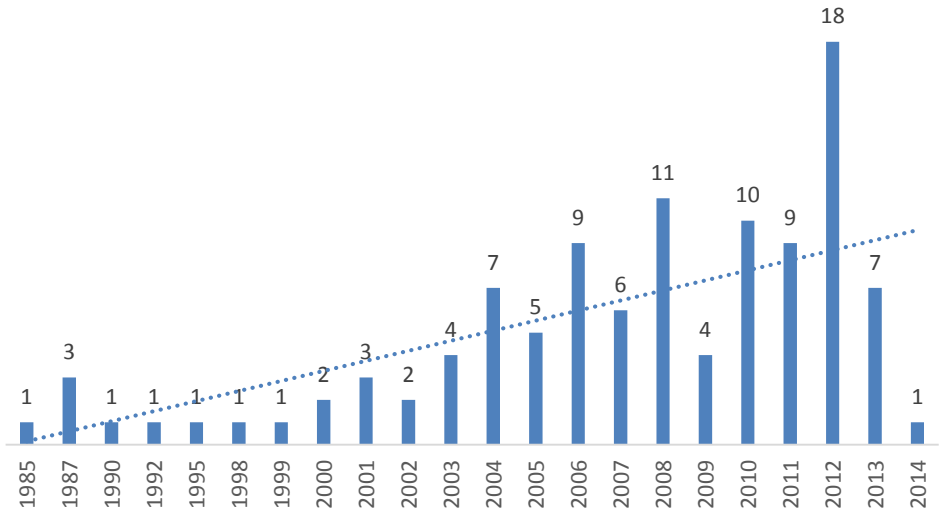


Figure 4 DoDI 8500.01 Policy Appendices Update **(DoD CIO 8500.01, 2014, pp. 8-13)**

Combining Figure 3 and 4 and looking at the cumulative effects, it becomes clear that leadership is adapting to the situation as threats emerge, more policy and guidance is added each year reacting to the threats presented.

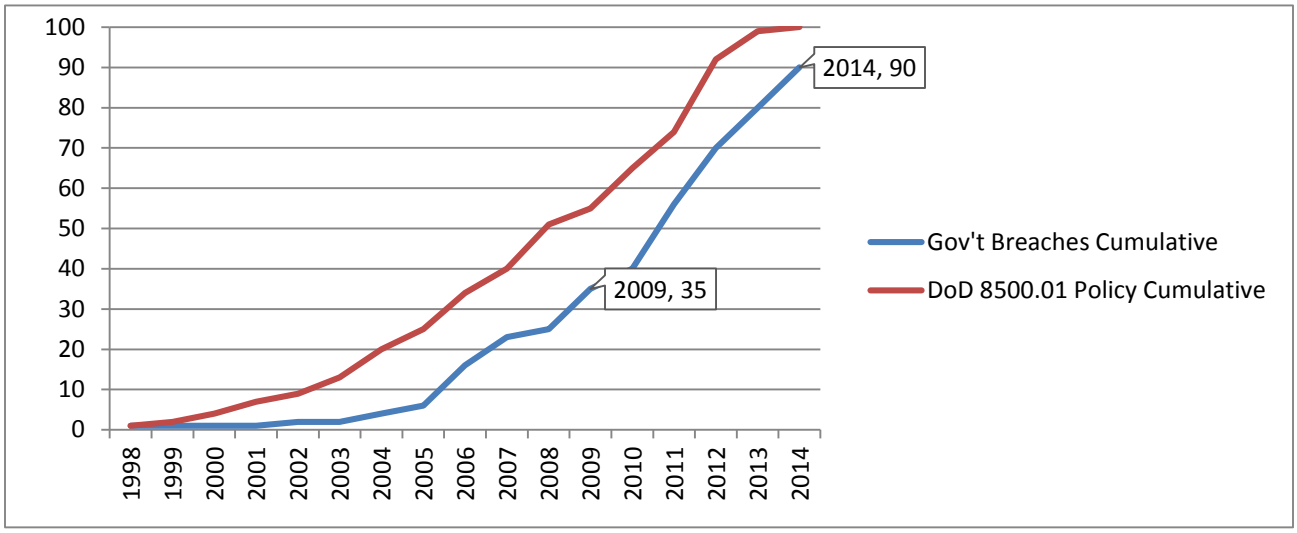


Figure 5 Combined Cumulative Breaches across U.S. Government and DoDI 8500.01

The continued increase in U.S. Government breaches, presents the image that these policies are not effective at deterring or minimizing the risks associated with cyber security breaches.

Cyber Physical System Research

Tactical Wheeled Vehicles (TWV) are multipurpose or special purpose military wheeled platforms that transport personnel and all classes of supply. They perform general or specific missions, and support all warfighting functions (Movement and Maneuver, Intelligence, Fires, Sustainment, Command and Control, and Protection). They are specially designed vehicles, or commercial vehicles modified to meet certain military requirements (Army G8, 2010, pp. B-4). Line-Haul Family of Vehicles (FoVs) are used in Army Transportation and Quartermaster units for transport of bulk supplies from air and sea ports to division support areas within a theater of

operation (Army G8, 2010, p. 11). The Army is evaluating the use of these systems for Autonomous and Semi-Autonomous Systems and Operations/ Manned-Unmanned Teaming "…these technologies offer similar capabilities for ground-based systems across all warfighting functions. A promising application would be autonomous ground-based resupply, which could provide optionally manned vehicle capability." (ARCIC, 2014, p. 2) Within these the autonomous vehicle exists the need to have computational algorithms controlling physical components, such as steering, braking, and shifting the gears within a transmission. Cyber Physical Systems is an emerging field which within the defense department CPS has been identified as a gap that should be further evaluated.

> CPS science and technology are fundamental to at least three of these seven areas: Engineering Resilient Systems (expediting design and delivery of trustworthy, adaptable and affordable defense systems), Cyber (DOD operations in cyberspace), and Autonomy (autonomous systems to augment military operations) (Cyber Physical Systems, 2015, p. 2)

National Science Foundation defines Cyber-Physical Systems as

> ... engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will far exceed the simple embedded systems of today. (National Science Foundation, n.d.)

Also the National Institute of Standard (NIST) has a directorate developing a framework for Cyber Physical System defines CPS as "…engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components" and provides for the challenges ahead within the field that does not have

> … mature science to support systems engineering of high-confidence CPS, and the consequences are profound. Traditional analysis tools are unable to cope with the full complexity of CPS or adequately predict system behavior…. The challenges and opportunities for CPS are thus significant and far-reaching. New relationships between the cyber and physical components require new architectural models that redefine form and function. (NIST Directorate for Computer & Information Science & Engineering, 2016)

and presents a method for risk identification in the categories of Safety, Reliability, Privacy, Resilience, and Cybersecurity . (CPS PWG Draft Framework for Cyber-Physical Systems, Release 0.8 1, 2015, p. 75)

Figure 6 CPS Risk View

The Software Engineering Institute (SEI) has identified five areas of study that are essential to CPS identified below.

> "**Timing Verification** to guarantee that tasks in real-time systems complete within their deadlines….
> **Functional Verification** to ensure that software behaves as required. …
> **Probabilistic Verification** to maximize the likelihood that a CPS will meet its desired goals. …
> **Collaborative Autonomy** to optimize scalability, performance, and extensibility for autonomous systems by creating a portable, open-sourced, decentralized operating environment….
> **Self-Adaptation** to address the challenge of having cyber-physical systems that can quickly adapt to a variety of situations including environment changes, and malfunctions…" (Software Engineering Institue - Carnegie Mellon University, n.d.)

Another perspective on the CPS is represented within the construct of a workflow consisting of four components, Physical Process, Networking, Computing and Actuation that have specific security objectives, such as Confidentiality, Integrity, Availability, and Authenticity.

Within these, there are a series of identified attacks, such as Eavesdropping, Compromised-Key, Man-in-the-Middle, and Denial-of-Service Attacks. (Eric Ke Wang, 2010)

Cyber Security Impacts to Autonomous Tactical Wheeled Vehicles

> "Driven by functional requirements and fast moving markets, these systems are being designed and deployed quickly. The design choices being made today will directly impact our nation's industries and critical infrastructure sectors over the next several decades….Modern vehicles are no longer purely mechanical systems,…Today's vehicles have interdependent cyber components used for telematics, conveniences, and safety-critical systems. A stealthy adversary could gain access to a vehicle's cyber components and remain completely hidden until initiating a widespread attack." (John Verrico, 2015)

Within the Department of Defense there is an on-going effort to demonstrate autonomy within ground truck systems known as Autonomous Mobility Appliqué System (AMAS) in response to user requirements (Theisen, Autonomous Mobility AppliquéSystem(AMAS) JCTD FY12-13 Industry Day, 2011). This system is comprised of hardware, software, sensors and network to support autonomous behavior, with the Hardware Concept identified in the figure below.

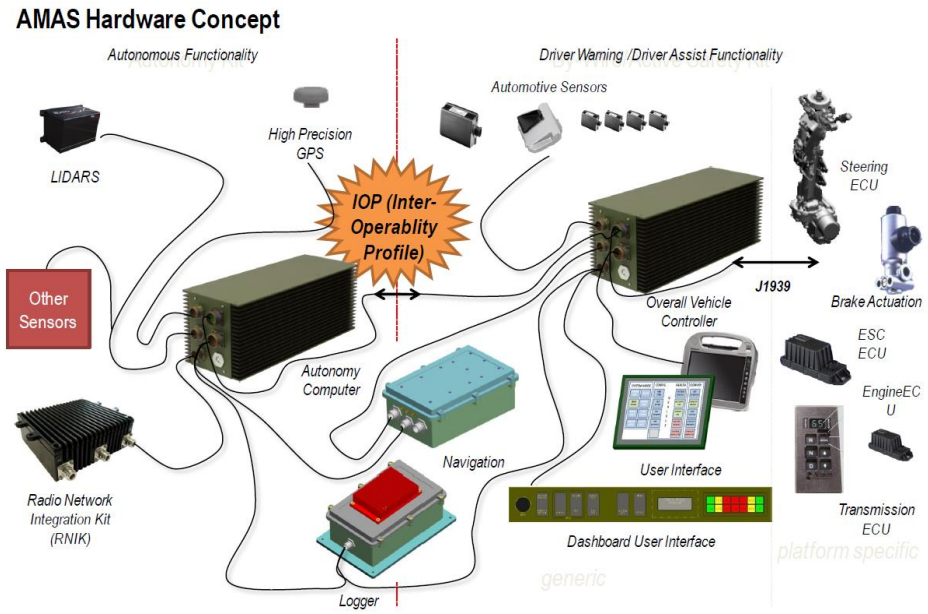


Figure 7AMAS Hardware Concept **(Bartz, 2013, p. 11)**

Within this architecture there exists commercial standards, such as CAN J1939, Gigabit Ethernet, and Flex Ray to support the interface between the Autonomous and Driver Warning/Driver Assist Functionalities as shown in the figure below.

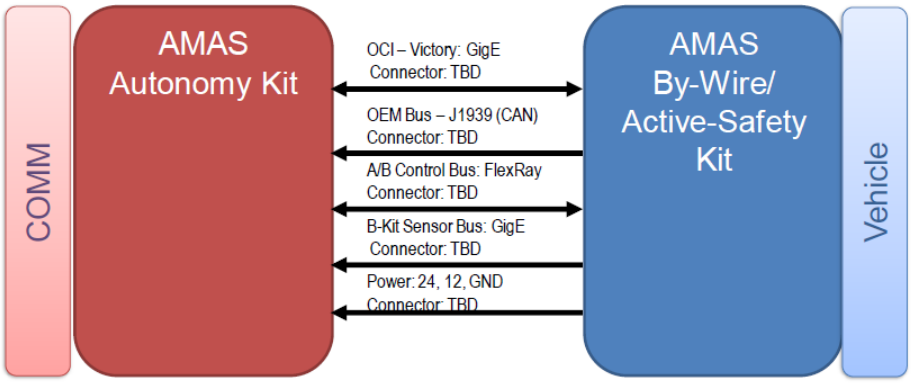


Figure 8AMAS Architecture **(Bartz, 2013, p. 7)**

The automotive vehicle CAN network has been demonstrated repeatedly to have risks associated with both physical access and remote injection of messages that alter vehicle systems performance (Chris Valasek, 2015). As demonstrated in Figure 9 below, there are many similarities between the architecture in the automotive segment as there is within the AMAS designs.

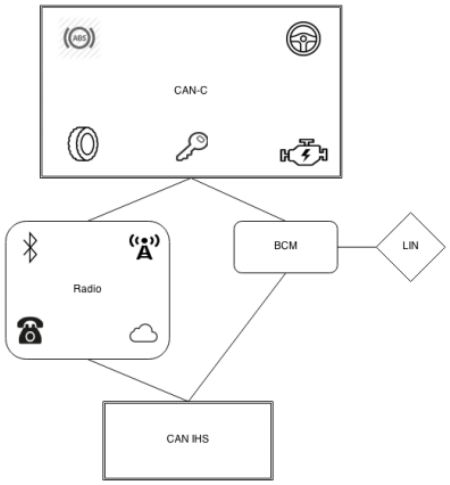


Figure 9 Jeep Cherokee Architecture Diagram **(Chris Valasek, 2015, p. 8)**

Within the Jeep Cherokee there are various cyber physical features that have been previously leveraged in attacks to gain access to physical capabilities of the automobile. Cyber physical systems, such as Adaptive Cruise Control, Forward Collision Warning, Lane Departure Warning, Park Assist, Tire Pressure Monitoring Systems, and Telematics. These systems all have a broad range of automotive attacks that can disable the engine control, provide remote access and control of various automotive vehicle systems (Chris Valasek, 2015).

Chapter 3 – Research Methodology

This study assessed the ability of PMs to manage cyber security risks on ground vehicles, and determined if awareness of what has increased since Boyd's study (Boyd, 2008). The study reviewed current Cyber Security policy and generated a timeline related to the policy creations in comparison to cyber incidents to identify how the policies have impacted the reoccurrence of cyber incidents. As the commercial truck industries innovate in the field of autonomy, these innovations will migrate into the Army autonomous tactical wheeled vehicles, As the hardware and software needed to enable these capabilities is integrated onto Army autonomous tactical wheeled vehicles, it is crucial that risks, specifically cybersecurity risks be addressed given that much of the commercial technology may be developed using globalized contractors. Moreover, with the recent increases in cyber incidents and the Army moving into autonomous tactical wheeled vehicles, the researcher wanted to identify to what degree the existing policy related to platform information technology (PIT) describes the systems in Army PM Systems and does cyber physical systems be a more appropriate term in support of autonomous tactical wheeled vehicles systems. Lastly look to merge the various methods to facilitate developing a method to generate Requirements for autonomous tactical wheeled vehicles.

Research Process

The survey instrument was initially reviewed within SSCF cohorts to check the questions for clarity and reliability. A second review was conducted by LTU professors. The survey was administered using Survey Monkey, with a link emailed to each Army PM with a digital signature to verify that the email was sent from an authorized DoD Enterprise email address.. The literature review was conducted using the resources available at the Lawrence Technological University (LTU) library. A review of the existing Department of Defense Instruction 8500.01 and 8510.01

on Cybersecurity was conducted and was used to evaluate the description of how Platform Information Systems are described, and the references increased over the years and compared to historical open source publicly available Federal Government cyber breaches.

Validity of the Research

This study does not have a hypothesis that requires research variables. The research surveyed 168 Army PMs on their perspectives regarding the globalization of their contractors, and the risks associated with using a globalized contractors in various categories available in Appendix A. There were 38 responses to the survey. Five were removed for insufficient responses, resulting in the 33 completed responses analyzed in Chapter 4.

Reliability of the Responses

The survey questions were reviewed by Lawrence Technology University professor Dr. Cole, and two initial sample surveys conducted with Senior Service College Fellows. Comments and revisions to question clarity, purpose and intent were revised during the two initial surveys. The questions provided a five point Likert scale, which contains various biases based on the sample surveyed (Wikipedia, 2016).

Data Collection

Data was collected using Survey Monkey online survey tool Assessment of the level of each perceived agreement on risk associated using a globalized contractor and the increased risk associated with software or hardware development. Other areas included the possibly increased risk associated with using foreign nationals. The Army PMs were asked if they strongly agreed, agreed, neither agreed/disagreed, disagreed or strongly disagreed with the perceived of using a globalized contractor. As the survey was Web-based it was designed to be easily accessed by the

PMs. A limitation using web-based surveys could be the specific browser used to run the survey, Army network filtering of Uniform Resource Locator (URL) that then needs to be copied and pasted into the browser window and the availability of PMs to take the short survey. Also the perception of clicking on an embedded link from an Army email address that was foreign to many may have limited responses to the survey. The survey questions were derived from Boyd's 2008 study on globalization, with the inclusion of the term cyber security, as it relates to the risks using globalized contractors The initial request went out in individual emails to each of the 168 Army PMs on 25 November 2015. A follow up email was sent 11 December 2015, with a final thank you and last chance email sent 14 December 2015.

Chapter 4 – Findings

Research Questions

1. Has the perception of cyber security risks increased since the 2008 study on software, hardware and supply chain risk?
2. Do program managers have the resources AUTHORITY AND SUPPORT to support cyber security requirements related to the Information system security manager (ISSM),
3. What challenges do PMs perceive with reciprocity related to cyber security?
4. What do Army PMs think opportunities are to obtain reciprocity with other PMs?

Population & Sample Size

The email distribution of Army PMs contained 168 total individuals, of which 38 (22.6%) initiated the online survey. Of the 38 that submitted a survey, five were removed because they had not answered a sufficient number of questions leaving 33 (20%). Comparatively, Cliff Boyd, received a total of 112 response from 205 PMs (54%) This delta may be explained given his method of having a General Officer request Army PMs perform the survey instead of an email requesting support for the research.

Collected Data

Research Question One

The survey repeated questions 3, 5, 6,7,8,9 and 10 from Boyd's study in 2008. The corresponding questions within this study are 7,8,9,13,14, and 15. Both studies asked respondents to provide answers either "strongly agree", "agree", "neither agree/disagree", "disagree" or "strongly disagree" to each of the questions presented. In his study, Boyd combined the count of responses in the categories of "strongly agree" with "agree" (SA/A), and "disagree" and "strongly disagree" (D/SD) to perform his analysis. He used the percentage of the responses in the three (SA/A), "Neither Agree nor Disagree" and (D/SD) in his analysis. To compare results from this study with

his, (Boyd, 2008, p. 42) the same process was used in this study. Comparing the results shown in Table 2 below with his Table 10 (Boyd, 2008, p. 42), there is a shift in the risk perceptions from Army PMs regarding the impact of using globalized contractors. In all but two questions, the Army PMs strongly agree or agree that the risk of using a globalized contractor. The risks increased between 4% and 23% respectively. There were two cases where there was a slight decrease in the risks - risk due to language differences decreased by 1% and Risk due to political issues decreased 5%.

Table 2 Survey Results from 2008 (Boyd, 2008, p. 42) & 2015

Globalization Impacts	2008-%Strongly Agree or Agree	2015-%Strongly Agree or Agree	2008-%Neither Agree Nor Disagree	2015-%Neither Agree Nor Disagree	2008-%Strongly Disagree or Disagree	2015-%Strongly Disagree or Disagree
Cost/Schedule risk due to export and import controls	55%	72%	32%	17%	12%	11%
Technical data protection	71%	83%	20%	14%	8%	3%
Cost/Schedule risk due to Buy American legislation / Cyber Policy(20	58%	81%	29%	11%	12%	8%
Program disruption at foreign sites	32%	36%	45%	44%	22%	19%
Obtaining state of the art technology due to export and import control	41%	53%	33%	31%	26%	17%
Obtaining state of the art technology due to emphasis on producing in	39%	58%	34%	28%	27%	14%
Software security and integrity due to offshore producer	60%	67%	27%	19%	13%	14%
Software security and integrity due to foreign nationals	54%	61%	32%	31%	14%	8%
Software security and integrity due to use of COTS SW	58%	69%	27%	25%	14%	6%
Raw material availability*	44%	not asked	39%	not asked	17%	not asked
Production risks from offshore producers	57%	73%	31%	24%	12%	3%
Integration when hardware produced by both U.S. and foreign sources	55%	76%	27%	18%	18%	6%
Supply chain disruption	62%	67%	17%	24%	20%	9%
OCONUS fielding using foreign nationals	34%	48%	42%	33%	24%	18%
Risk due to language differences	37%	36%	30%	39%	34%	24%
Risk due to political issues	50%	45%	31%	48%	19%	6%
Risk due to legal differences	56%	64%	26%	33%	18%	3%
Risk due to cultural differences and flashpoints	43%	50%	32%	41%	25%	9%
Risk due to geographically dispersed workforce	42%	55%	35%	29%	22%	16%

Table 3 Delta between 2008 (Boyd, 2008, p. 42) and 2015 Army PM responses

Globalization Impacts	Delta - Strongly Agree or Agree	Delta - % Neither Agree Nor Disagree	Delta Disagree/Strongly Disagree
Cost/Schedule risk due to export and import controls	17%	-15%	1%
Technical data protection	12%	-6%	5%
Cost/Schedule risk due to Buy American legislation / Cyber Policy(2015)	23%	-18%	4%
Program disruption at foreign sites	4%	-1%	3%
Obtaining state of the art technology due to export and import control	12%	-2%	9%
Obtaining state of the art technology due to emphasis on producing in U.S.	19%	-6%	13%
Software security and integrity due to offshore producer	7%	-8%	-1%
Software security and integrity due to foreign nationals	7%	-1%	6%
Software security and integrity due to use of COTS SW	11%	-2%	8%
Production risks from offshore producers	16%	-7%	9%
Integration when hardware produced by both U.S. and foreign sources	21%	-9%	12%
Supply chain disruption	5%	7%	11%
OCONUS fielding using foreign nationals	14%	-9%	6%
Risk due to language differences	-1%	9%	10%
Risk due to political issues	-5%	17%	13%
Risk due to legal differences	8%	7%	15%
Risk due to cultural differences and flashpoints	7%	9%	16%
Risk due to geographically dispersed workforce	13%	-6%	6%

The two questions had an increased perception of risk by at least 20%. The first was the cost/schedule risk due to buy American legislation, and the second was the Integration risk when hardware is produced by both U.S. and foreign sources. The cost/schedule risk due to buy America, could be explained by the reason that many of the technologies are no longer produced within the United States. Therefore causing the Army PMs to request waivers to the policy and increase cost and schedule within their programs to execute the additional steps to obtain the products from a source outside the U.S. The second regarding the integration of hardware produced by both U.S. and foreign sources, could be that since the hardware is produced and procured from outside the U.S., there is a possibility that risks are introduced through the international supply chain as the hardware is handled through the supply chain. Alternatively, it is also plausible that differences in standards, laws, regulations and prohibited materials vary

significantly. This can cause delays in obtaining waivers to use materials or products that are restricted for various reasons within the U.S.

Within each of these questions is an area of risk associated with the development of autonomous tactical wheeled vehicles. The discussion of cost risks driving the U.S. defense companies to seek work in the global economy, drives offsets that contractually bind them to perform in the foreign country possibly sharing U.S. technical data. The ability to protect technical data by a U.S. defense contractor engaged in offsets that require a joint venture, in which they are the minor shareholder of the foreign owned company and do not have the authority to secure the technical information, as required by U.S. DoD Standards. Disruptions at foreign sites could expose U.S. defense hardware and software to additional cyber risks as there is a potential for theft and sale to other nation states. Development of software and hardware offshore, by foreign nationals, or foreign COTS makes the hardware and software available to foreign adversaries that could introduce risks into the system components. Language and political differences can affect the legal understanding of what offsets are required and how offsets are managed by U.S. defense companies or the local joint venture performing in a global economy to support the U.S. acquisitions of systems for use in autonomous tactical wheeled vehicles. A geographically dispersed workforce presents both physical and cyber security risks at each of the sites potentially making U.S. technical information available to foreign adversaries or provide a means to introduce risks into the systems that could be used to achieve autonomy for the tactical wheeled vehicles.

perceptions by Army PMs align with the U.S. defense contractors risk reporting in their business planning documents (GENERAL DYNAMICS CORPORATION, 2014) (UNITED TECHNOLOGIES CORP, 2015) (RAYTHEON COMPANY, 2015) (NORTHRUM

GRUMMAN, 2015). These perceptions continue to exist and are a risk to the development of the various technologies that would be integrated into an autonomous tactical wheeled vehicles. The development of the various systems to enable autonomy appear to lie within the span of a single Program Executive Office within the Army. However the external communication mechanisms that allow the autonomous tactical wheeled vehicles to communicate to the tactical network exist within a different Program Executive Office (Tourner & Clow, 2016). These differences in perception of risks using a globalized contractor by Army PMs, the declining defense budgets (Kevin Dehoff, 2013) to develop the technology for the department of defense, shifting from defense purpose built to commercially developed and modified for defense (Fahey, 2015), the U.S. defense contractors own admission of inherent risk from offsets (GENERAL DYNAMICS CORPORATION, 2014) (UNITED TECHNOLOGIES CORP, 2015) (RAYTHEON COMPANY, 2015) (NORTHRUM GRUMMAN, 2015), a new initiative to reduce systems acquisition costs thru international programs and interoperability (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, n.d.) and the lack of impact of policy on decreased cyber breaches (Rosenzweig D. I., 2014) (Rosenzweig P. , 2012), point to an increasing risk in development of the technology systems and software that will be implemented in developing, manufacturing and fielding autonomous tactical wheeled vehicles.

Furthermore, Boyd's study also evaluated the formal training Army PMs (Boyd, 2008, p. 49) related to working managing risks with a globalized contractor and in his outcomes called for Defense Acquisition University (DAU) and Defense Acquisition Workforce Improvement Act (DAWIA) provide additional training, and support for working with and identifying risks when working with a globalized contractor. Providing and increasing training to Army PMs can facilitate awareness and greater understanding of the importance of ensuring a secure supply chain when

working with a globalized contractor. It appears these efforts have not either been implemented or have not been effective (Boyd, 2008, pp. 51,52). DAU has developed an International Acquisition Career Path (IACP) (DAU, n.d.) in response to guidance in DoD Directive 5000.01, DoD Instruction 5000.02 (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, n.d.). DAU's Int'l courses, such as ACQ 120, ACQ 130, and ACQ 230 address risk through some standard "the 5 phases" slides. DAU provides CLE 074 – Cybersecurity Throughout Acquisition which is not mandatory and three more courses forthcoming in 2016 (DAU , n.d.). It remains to be seen how these courses will impact the associated risks working with a globalized contractor and the overall associated risk to autonomous tactical wheeled vehicles.

Research Question Two

Department of Defense Instruction (DoDI) 8510.01 dated March 12, 2014, applies to

> All DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS [Information systems], platform IT (PIT), IT services, and IT products. This includes IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD. (DoD CIO 8510.01, 2014, p. 2)

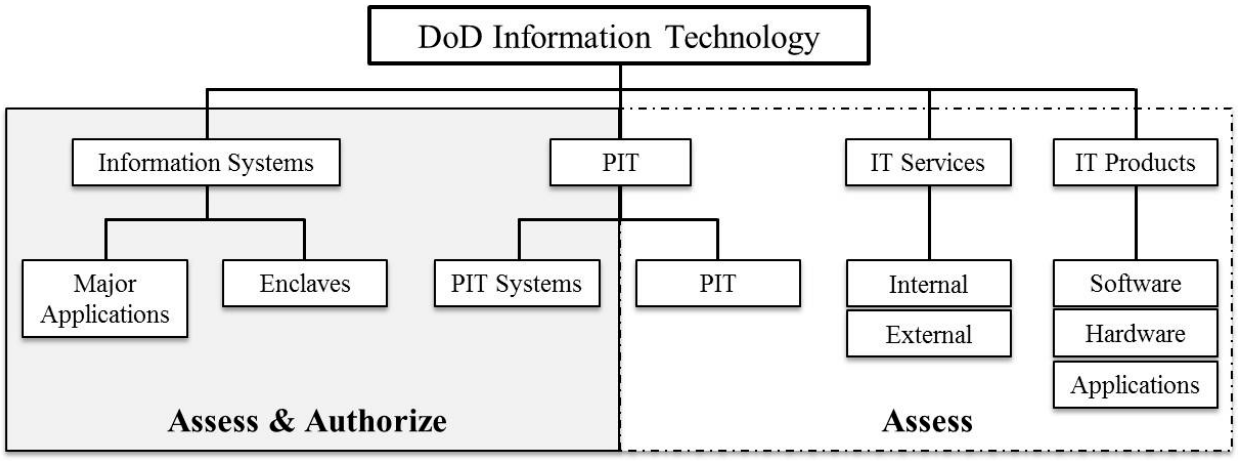


Figure 10 DoD IT (DoD CIO 8500.01, 2014, p. 12)

Within that framework platform information technology (PIT) applies to the systems identified within Figures 7 and 8 relative to the PIT required to support the implementation of the

requirements for autonomous tactical wheeled vehicles. Since the autonomous tactical wheeled vehicles will "…receive, process, store, display, or transmit DoD information.… And will require to undergo …development, test and evaluation (T&E)…" (DoD CIO, 2014, p. 2)

Moreover, DoDI 8510.01 states that Program Manages must

> 1. Appoint an ISSM for each assigned IS or PIT system with the ***support*** [emphasis added], ***authority***[emphasis added], and ***resources*** [emphasis added] to satisfy the responsibilities established in this instruction.
>
> 2. Ensure each program acquiring an IS or PIT system has an assigned IS security engineer and that they are fully integrated into the systems engineering process.
>
> 3. Implement the RMF for assigned IS and PIT systems.
>
> 4. Ensure the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process. (DoD CIO 8510.01, 2014, p. 18 Enclosure 4)

DoDI 8510.01 identifies the role of I[nformation] S[ystem] Security Manager (ISSM) that "…is responsible for ensuring all products, services and PIT have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system." (DoD CIO 8510.01, 2014, p. 12).

Furthermore the ISSMs, must:

> 1. Support implementation of the [Risk Management Framework] RMF.
> 2. Maintain and report IS and PIT systems assessment and authorization status and issues in accordance with DoD Component guidance.
> 3. Provide direction to the ISSO in accordance with Reference (h).
> 4. Coordinate with the organization's security manager to ensure issues affecting the organization's overall security are addressed appropriately. (DoD CIO 8500.01, 2014, p. 19)

And

> (1) Determine the security impact of proposed or actual changes to the IS or PIT system and its environment of operation. Included in the security controls assigned to all IS and PIT systems are security controls related to configuration

and deficiency management, performance monitoring, and periodic independent evaluations (e.g., penetration testing).

> (a) The ISSM, in coordination with other appropriate personnel (e.g., IS security engineer, system administrators, CNDSP):
>
> 1. Continuously monitors the system or information environment for security-relevant events and configuration changes that negatively affect security posture.
>
> 2. Periodically assesses the quality of security controls implementation against performance indicators, such as: security incidents; feedback from external inspection agencies (e.g., OIG DoD, Government Accountability Office (GAO)); exercises; and operational evaluations, including Director, OT&E IA, assessments.
>
> 3. Must report any significant change in the security posture of the system, and recommended mitigations, immediately to the SCA and AO.
>
> 4. May recommend to the SCA or AO a reassessment of any or all security controls at any time. (DoD CIO 8500.01, 2014, pp. 36,37)

Moreover in Department of Defense Instruction (DoDI) 8500.01 dated March 14, 2014 states that the

> ISSMs:
>
> a. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.
>
> b. Ensure that IOs and stewards associated with DoD information received, processed, stored, displayed, or transmitted on each DoD IS and PIT system are identified in order to establish accountability, access approvals, and special handling requirements.
>
> c. Maintain a repository for all organizational or system-level cybersecurity-related documentation.

> d. Ensure that ISSOs are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures such monitoring.
>
> f. Ensure that cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.
>
> g. Ensure implementation of IS security measures and procedures, including reporting incidents to the AO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures in accordance with Reference (bo) for classified information or Reference (bp) for CUI, respectively.
>
> h. Ensure that the handling of possible or actual data spills of classified information resident in ISs, are conducted in accordance with Reference (bo).
>
> i. Act as the primary cybersecurity technical advisor to the AO for DoD IS and PIT systems under their purview.
>
> j. Ensure that cybersecurity-related events or configuration changes that may impact DoD IS and PIT systems authorization or security posture are formally reported to the AO and other affected parties, such as IOs and stewards and AOs of interconnected DoD ISs.
>
> k. Ensure the secure configuration and approval of IT below the system level (i.e., products and IT services) in accordance with applicable guidance prior to acceptance into or connection to a DoD IS or PIT system. (DoD CIO 8500.01, 2014, pp. 49,50)

With roles and responsibilities outlined in the DoDI 8500.01 and DoDI 8510.01 for both the PMs and the ISSM, survey questions 11 and 12 were posed to the Army PMs. Question 11, asked if the PMs had an ISSM and were provided the responses of “Yes”, “No”, and “Unsure”. Question 12 measured if Army PMs strongly agreed, agreed, neither agree/disagree, disagree or strongly disagree that the ISSM has the responsibility, authority and support outlined in DoDI 8500.01 and DoDI 8510.01 detailed above.

The responses to question 11 were counted and turned to percentages and are provided in Table 4 below. The responses to question 12 were counted and combined for the strongly agree and agree, and disagree and strongly disagree, and converted to percentages for the sampled Army PMs with the results provided in Table 5 below.

Table 4 ISSM Assigned

ISSM:	Yes	No	Unsure
ISSM is assigned	64%	27%	9%

Table 5 ISSM Support, Authority and Resources

	Strongly Agree/Agree	Neither Agree or Disagree	Disagree/Strongly Disagree
ISSM has the SUPPORT	73%	15%	12%
ISSM has the AUTHORITY	70%	12%	18%
ISSM has the RESOURCES	45%	30%	24%

The respondents provided that 64% of them have an ISSM assigned, 27% did not have one and 9% were unsure. The Army PMs responded with their level of agreement or disagreement to question 12 providing that 73% strongly agree or agree that the ISSM has the SUPPORT they need to perform the responsibilities outlined, 70% strongly agree or agree that the ISSMs AUTHORITY to perform their responsibilities, and only 45% of the ISSMs have the RESOURCES to perform their responsibilities. So while the ISSMs have the authority and support, at least 24% of the Army PMs surveyed disagree or strongly disagree that the ISSM has the necessary resources to conduct their duties. This clearly presents not just a risk, but an issue, to autonomous tactical wheeled vehicles as the ISSMs are responsible for the efforts that should help to identify and mitigate the risks associated with the integration of the various software, and

hardware components that could be used to implement the autonomy desired by the Army (ARCIC, 2014) (Tourner & Clow, 2016).

Research Questions Three and Four

DoDI 8510.01 defines and provides the process for reciprocity as follows:

> Cybersecurity reciprocity (referred to in this instruction as "reciprocity") is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DoD Information Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources. The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation. In order to facilitate reciprocity, the concepts in paragraphs 1a through 1e are fundamental to a common understanding and must be adhered to:
>
> a. IS and PIT systems have only a single valid authorization. Multiple authorizations indicate multiple systems under separate ownership and configuration control.
>
> b. Deploying systems with valid authorizations (from a DoD organization or other federal agency) are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving enclave or site. Deploying system ISOs and PMs must coordinate system security requirement with receiving organizations or their representatives early and throughout system development.
>
> c. An authorization decision for IS or PIT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations must provide the complete security authorization package to receiving organizations. PMs/ ISOs deploying systems across DoD Components will post security authorization documentation to Enterprise Mission Assurance Support Service (eMASS) or other electronic means to provide visibility of authorization status and documentation to planned receiving sites.
>
> d. The process for receiving organization to accept IS and PIT systems is:
>
> (1) Review the complete security authorization package.
>
> (2) Determine the security impact of connecting the deploying system within the receiving enclave or site.

> (3) Determine the risk of hosting the deploying system within the enclave or site.
>
> (4) If the risk is acceptable, execute a documented agreement between deploying and receiving organizations (e.g., memorandum of understanding (MOU), memorandum of agreement (MOA), SLA) for the maintenance and monitoring of the security posture of the system (security controls, computer network defense service provider (CNDSP), etc.).
>
> (5) Document the acceptance by the receiving
>
> (6) Update the receiving enclave or site authorization documentation for inclusion of the deployed system.
>
> e. Receiving organizations have the right to refuse deploying systems due to a security authorization package that does not meet sufficiency and completeness requirements as defined on the KS, or excessive risk to the enclave or site, as determined by the enclave or site AO. Refusals must be documented by the refusing AO, and provided to the deploying organization's ISO or PM, AO, and Component SISO, and to the refusing organization's Component SISO. Disputes should be resolved at the lowest possible level. Disputes that cannot be resolved will be raised to the next appropriate level (e.g., DoD Component, MA PAO, DSAWG, DoD ISRMC). (DoD CIO 8510.01, 2014, pp. 21,22)

Since autonomous tactical wheeled vehicles will likely be integrating systems from various IT or PIT systems, it was essential to ask the Army PMs perception on achieving the defined reciprocity defined above. Questions 10.d and 40 were asked in the survey on relating to reciprocity. Question 10.d asked Army PMs to provide their level of agreement that reciprocity would be simple to obtain responding either strongly agree, agree, neither agree or disagree, disagree or strongly disagree. Question 40 was left as an open response question asking Army PMs for areas where opportunities for reciprocity could be achieved with other PMs on Cyber Risks. Responding to question 10.d that reciprocity agreements will be simple to develop the

Army PMs responded that 36% disagree or strongly disagree, 47% were neither agreed nor disagreed and only 17% strongly agreed or agreed that they would be simple to develop.

Table 6 Reciprocity Agreements

	Strongly Agree/Agree	Neither Agree or Disagree	Disagree/Strongly Disagree
Reciprocity agreements will be simple to develop	17%	47%	36%

Reciprocity is essential to the integration of various enabling systems onto a platform information technology (PIT) systems, illustrated by Figures 7 and 8, components that are essential in enabling autonomous tactical wheeled vehicles. Again as DoDI 8501.01 states "…reciprocity reduces redundant testing, assessing and documentation, and the associated costs in time and resources. The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation" (DoD CIO 8510.01, 2014, pp. 21, Enclosure 5) Developing the reciprocity agreements becomes an entangled challenge as Commercial Off the Shelf (COTS) components are used. COTS products may not have the same rigorous testing perform as purpose built military components. Because reciprocity requires the accepting organization to review, the "…authorization decision for IS or PIT system cannot be made without completing the required assessments and analysis, as recorded in the security authorization package. Deploying organizations must provide the complete security authorization package to receiving organizations…" (DoD CIO 8510.01, 2014, pp. 21, Enclosure 5). The receiving organization then has to assess the risks associated with integrating the provided sub-system or component into their own system. The receiving organization can reject the provided component should the risk be unacceptable by the receiving office action officer. Moreover if the various systems are developed by globalized U.S. Defense contractors and a reciprocity

agreement existed for a component that was developed overseas by a foreign national the risk could be acceptable by the providing organization, however the receiving organization may determine the risk is too high and reject the provided system component. As 8510.01 states the "Receiving organizations have the right to refuse deploying systems due to a security authorization … excessive risk to the enclave or site, as determined by the enclave or site AO." (DoD CIO 8510.01, 2014, pp. 21, Enclosure 5). All this assumes that there is an action officer or an ISSM that has the authority, support and resources to make execute the policy steps and procedures.

Given the challenges with reciprocity outlined above, the researcher was interested in hearing if the Army PMs had any insights on opportunities to achieve reciprocity. Question 40 was an open responses in the survey asking what are the opportunities to attain RECIPROCITY with other PMs on Cyber Risks? Twelve responses were submitted and generalized by the researcher. The responses stated that there was none or unknown methods and one response provided recommended cost sharing on known or shared risks. It could be that the process outlined above and the relatively new creation of both DoDI 8500.01 and DoDI 8510.01 has not made its way into the Army PM training curriculum and therefore not a subject some or many are familiar with.

Open Ended Questions

Lastly, the survey asked Army PMs one additional open ended question and provided a field for any additional comments. The question was "What areas do you perceive need Cyber Security support?" One response that the researcher found interesting follows:

> In my office of 244 personnel, I have 2 people I consider experts, and another 5-6 that have a good understanding of Cyber. The rest of us know next to nothing. It may be

> beneficial for DAU to develop some course material that provides a general understanding for the majority of PMs, engineers, and logisiticians<sic>--rather than the tendency to just focus on better training the narrow stovepipe of individuals who focus on it (though we need that too) (Anonymous Army PM)

This anonymous response was reinforced by the Army PMs response to question number 34 of the survey. Question number 34 asked "Which of the following learning objectives and/or learning opportunities should be included in ANY formal training classes to address the risk posed when using a globalized contractor?" The results were counted, converted to percentages and are presented in table 7 below. 64% of the Army PMs felt that Cyber Security should be included in current and future training opportunities when a globalized contractor is part of the subject training provided.

Table 7 Training to be included when discussing a globalized contractor

Subject to Include in Training w/ Globalized Contractor	Percent
Cyber Security	64%
Export/Import Regulations, Laws, and Processes	42%
U.S. Production Policies Affecting DoD	39%
International Business and Contracting Introduction	24%
Impacts of Globalization	15%
Introduction to international law	15%
Understanding what is Globalization	12%
Global Economics	12%
Utilizing industry globalization training	9%
Causes of Globalization	6%

Chapter 5 – Conclusions and Recommendations

The cyber security strategies recommend working with commercial markets to support cyber security improvements in DoD and Federal systems (The White House;Office of the Press Secretary, 2015) (Carter, 2015). In chapter four the survey responses identify an increased awareness of the risks when using a globalized contractor. Furthermore the decreasing DoD Budget has increased the need of U.S. Defense contractors to shift to foreign markets and falls within the definition of a 'globalized contractor'. These foreign markets, in many cases, require the use of offsets, which have increased over time. Moreover the U.S. Defense contractors may not be able to secure their intellectual property or systems in a foreign country which can lead to the introduction of risks into DoD products. Lastly, Army PMs felt that while their ISSMs have the authority and support, the ISSMs do not have the resources to carry out their roles and responsibilities as outlined in the DoDI 8500.01.

Recommendations

The following three recommendations will be discussed in this section.

1. Establish an Autonomous Consortium
2. Revise DoDI 8500.01
3. Prioritize Cyber Within DoD Planning, Programming, Budgeting and Execution Process (PPBE)

Establish an Autonomous Consortium

Given the previous discussions and the magnitude of the effort it has become essential to engage with the commercial, academic, non-standard defense companies, small businesses and

federal groups to address the impacts of autonomy in both the commercial and defense industries. Governor Snyder in his 2016 State of the State discussed the transformation of the automotive industry into the mobility industry and that 70% of the research and development for the U.S. automotive industry is done in the State of Michigan. The State of Michigan created in partnership with the University of Michigan and host of partners the Michigan Mobility Transformation Center and is creating the American Center for Mobility (Snyder G. R., 2016, pp. 8,9). This presents a keen opportunity for the centrally located Tank Automotive Command (TACOM) in Warren Michigan. As President Obama discussed, the need to partner with the commercial and local governments makes it essential that DoD needs to be an integral partner within this new American Center for Mobility, to develop not only the autonomy vehicle system standards that will benefit both commercial and defense, but also the means to test, verify and validate the true risks. This presents a challenge given that many of the partners within this center will likely not be able to do business with DoD given the typical Federal Acquisition Regulations that come with a high cost of entry. However, the National Defense Authorization Act for Fiscal Year 2016 provides on pages 47 and 48 "SEC[TION]. 218. DEPARTMENT OF DEFENSE TECHNOLOGY OFFSET PROGRAM TO BUILD AND MAINTAIN THE MILITARY TECHNOLOGICAL SUPERIORITY OF THE UNITED STATES." To

> …establish a technology offset program to build and maintain the military technological superiority of the United States … would help counter technological advantages of potential adversaries of the United States, including…**autonomous systems…cyber technology**[emphasis added]…developed using research funding of the Department of Defense and accelerating the commercialization of such technologies; and (B) developing and implementing new policies and acquisition… the purposes for which such a department, agency, or command may apply for funds and appropriate requirements for technology development or commercialization to be supported using program funds…applications for funding to be used to enter into contracts, cooperative agreements, or o**ther transaction agreements** [emphasis added] entered into pursuant to section 2371b of title

> 10, United States Code, as added by section 815,with appropriate entities for the fielding or commercialization of technologies…for fiscal year 2016 for research, development, test, and evaluation, Defense wide, not more than $400,000,000 may be used for each such fiscal year for the program established under subsection… (House of Representative 114TH CONGRESS, 2015, pp. 48,49)

These Other Transaction Agreements (OTA) are identified in Section 2371b of Title 10 which simplifies working with the department of defense and enable to provide the assistance to benefit a public purpose, which reduces the overhead from FAR contracts and the regulations that typically limit the ability of non-standard defense companies to work with the DoD (Aerospace Industries Association of America, Inc., 2011). This section supports entering into transactions (other than contracts, cooperative agreements and grants) with any other department or agency of the Federal Government, to perform the work described and needed supporting autonomy and cyber security.

"The Defense Department has benefited from private sector innovation throughout its history. Going forward, DoD will work closely with the private sector to validate and commercialize new ideas for cybersecurity for the Department" (Carter, 2015, p. 4). leveraging the desire by the Governor of Michigan, the existing commercial base within the State of Michigan and the alignment of commonality between the Army's needs for autonomous systems, reducing DoD budgets and the need for reducing the cyber security risks its critical to leverage the OTA to enter into the budding field where autonomy and cyber security become a cohesive element within commercial and defense products. This consortium could help offset the lack of resources the ISSMs have within the Army PMs offices to support risk reductions to autonomous systems and the cyber security impacts that would be identified shared across the spectrum of autonomous systems possibly beyond ground systems.

Revise to DoDI 8500.01

Presented within DoDI 8500.01 there exists the term Platform Information Technology, or Platform IT or PIT. These may have a better relationship to the specific terminology of information technology and may not properly describe the future of autonomous systems moreover how they have impacts to the physical world. Typically information technology is perceived as ones and zeros within a computer that don't or can't impact a physical object. This perception has to shift,

> We live in a wired world. … Computer code blurs the line between the cyber and physical world and connects millions of objects to the Internet or private networks. (Carter, 2015, p. 1)

When evaluating the definitions proposed for and methods used to describe PIT systems, they all trace back to IT standards. As an example within DoDI 8500.01 it states

> "(a) All PIT has cybersecurity considerations. The Defense cybersecurity program only addresses the protection of the IT included in the platform. See Reference (q) for PIT cybersecurity requirements." (DoD CIO 8500.01, 2014, p. 39)

and

> "1. PIT systems are ***analogous to enclaves*** [emphasis added] but are dedicated only to the platforms they support. PIT systems must be designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems."

Defining enclaves as

> "1. Enclave
> a. Enclaves provide standard cybersecurity, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.
>
> b. Enclaves always assume the highest security category of the ISs that they host, and derive their security needs from those systems. See

> Reference (ch) for a discussion of IS boundaries and the application of security controls." (DoD CIO 8500.01, 2014, p. 38)

and

> "3. Although other federal departments and agencies may treat PIT systems as a type of IS, DoD platforms supporting certain DoD missions have unique operational and security needs." (DoD CIO 8500.01, 2014, p. 40).

The references to further detail PITs reach into the DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 (q) and Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, as amended (ci) to further help define and categorize PIT systems.

Within the Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 15, 2012, states the target audience

> …serves the national security community's information security and information assurance (IA) professionals, including those responsible for—
>
> • Information systems, information security, or risk management and oversight (e.g., Chief Information Officers [CIO], Risk Executive (Function), Senior Information Security Officers [SISO], and Authorizing Officials)
>
> • Information system development (e.g., program and project managers, mission/application owners, system designers, system/application programmers, Information Security Systems Engineers [ISSE], and Information Security Architects)
> • Information security implementation and operation (e.g., information system owners, data stewards, ISSEs, information system administrators, Information System Security Officers [ISSO], and Information System Security Managers [ISSM])
>
> • Information system and information security assessment and monitoring (e.g., auditors, Inspectors General [IGs], evaluators, ISSOs, and assessors). (PLUNKETT, 2012, p. 2)

And within the DoDI 8510.01 provides for the assignment of roles and responsibilities of PIT systems and provides for the application of the Risk Management Framework to PIT systems showing in Figure 10 below.

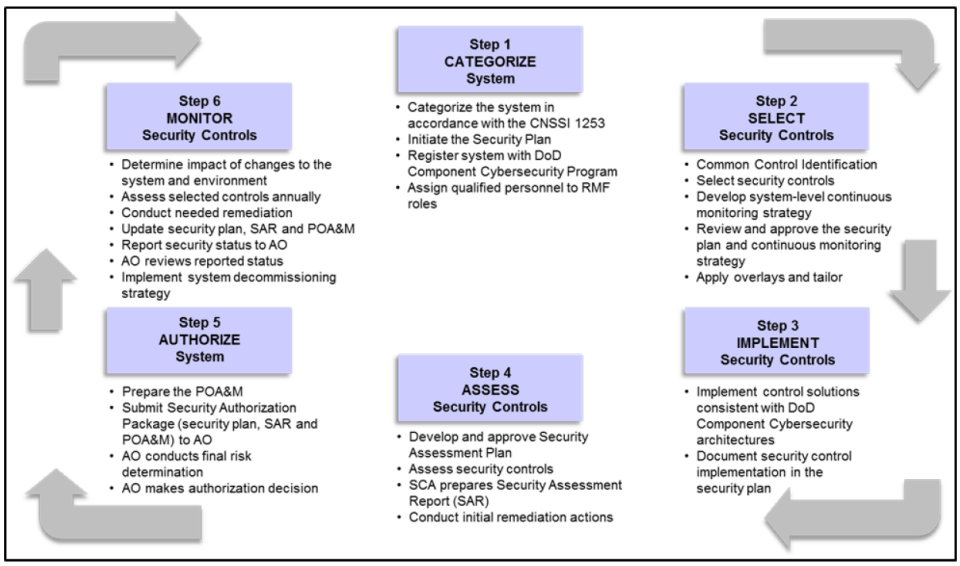


Figure 10 Risk Management Framework for IS and PIT (DoD CIO 8510.01, 2014, p. Enclosure 6 pg 28)

As such the language used to describe the interaction between the physical and cyber should introduce Cyber Physical Systems (CPS) as an element of DoDI8500.01. As discussed in the literature review there's significant gaps within this arena that the commercial and academia have begun and will continue to expand and grow. Aligning DoD instructions now to these new terms appears to be a minor shift, however, the impact is significant. As we've all been told, that "Words have meaning", it is never truer than in this case. The literature review discussed the lack of Cyber Physical System (CPS) research within the various federal departments, and with the desire to migrate into the autonomous tactical wheel vehicles it is essential that the terminology be introduced into the Department of Defense. The definition of CPS includes the physical

aspect and controls for that physical environment. This is key in enabling the various elements required to determine if a system has been negatively compromised. A method of determining if a system is compromised could be the physical response that a sensor perceives or a camera inspects. The methods increase dramatically when shifting beyond just the information technology aspects of the words.

The research proposes to therefore include the word Cyber Physical Systems, leveraging the definition from the National Science Foundation: "Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components." (National Science Foundation, n.d.). This would apply to many of the systems that would be required to enable autonomous capabilities within the tactical wheeled vehicles. Moreover attempting to introduce information technology standards to a real time system such as an engine or transmission controller, or the anti-lock brakes may prove dangerous.

Lastly, given the recently published Society of Automotive Engineers (SAE) standard J3061 titled "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" which

> …provides guidance on vehicle Cybersecurity and was created based off of, and expanded on from, existing practices which are being implemented or reported in industry, government and conference papers. The best practices are intended to be flexible, pragmatic, and adaptable in their further application to the vehicle industry as well as to other cyber-physical vehicle systems (e.g., commercial and military vehicles, trucks, busses). This recommended practice establishes a set of high-level guiding principles for Cybersecurity as it relates to cyber-physical vehicle systems.
>
> This includes:
>
> • Defining a complete lifecycle process framework that can be tailored and utilized within each organization's development processes to incorporate Cybersecurity into cyber-physical vehicle systems from concept phase through production, operation, service, and decommissioning.

> • Providing information on some common existing tools and methods used when designing, verifying and validating cyber-physical vehicle systems.
>
> • Providing basic guiding principles on Cybersecurity for vehicle systems.
>
> • Providing the foundation for further standards development activities in vehicle Cybersecurity. The appendices provide additional information to be aware of and may be used in helping improve Cybersecurity of feature designs. (SAE, 2016)

further strengths the case to shift with industry.

Prioritize Cyber Within DoD Planning, Programming, Budgeting and Execution (PPBE) Process

DoD has prioritized $7 billion dollars for the 2017 budget to enable DoD Network defenses, additional training and developing cyber tools and infrastructure for offensive cyber operations with the DOD CIO's 2016 budgets included a $5.5 billion request for cyberspace operations (Lyngaas, Pentagon Chief: 2017 budget includes $7B for cyber, 2016). The U.S. has become reliant on technologies that provide the the U.S. military strengths but may introduce vulnerabilities that adversaries can exploits (Lyngaas, Pentagon Chief: 2017 budget includes $7B for cyber, 2016).

As the Army PMs identified, they perceive a lack of resources exist to support the ISSMs in execution of their role. As such the PPBE process should prioritize cyber requirements as a high priority within the planning and program elements to enable the Army PMs to execute polices that have been published. As the shown in the literature review in chapter 2 regarding the growing number of breaches and the policies following retroactively, one plausible reason for the continued growth of breach is the lack of funding to support the cyber policy and implement safe guards. The lack of safeguards as the Joseph Dunford, Chiarman of the Joint Chiefs of Staff recently stated,

“We...need to develop a framework within which to deter cyber threats, and obviously attributing threats and managing escalation and hardening ourselves against cyberattacks are all areas that require more work…having the tools to implement that, those are all different things,"” (Lyngaas, Dunford: U.S. has work to do in cyber deterrence, 2016).

Thus it is essential that Army PMs have a means to prioritize their resourcing needs for their ISSM to execute the policies that are met to safeguard military systems for cyber threats.

Conclusions

As the research identified the increasing globalization of the US defense industry driven by the declining US defense budget. This continued globalization has created the opportunity in foreign nations has led to an increasing demand for offsets. Moreover the continued growth of cyber breaches within the Federal Government and the reactive response in policies have not had a significant impact on reducing the risks. Also as the policies are enactment and the research surveyed the Army PMs on one aspect of the policies, the information system security manager (ISSM). The Army PMs responded that while many have the individual role and support in place to enable execution of the policy only 45% responded that they have the resources, typically funding, to support the role. This leads to an increased level of risk within the Army as whole in this particular area of cyber. Furthermore, as the Army drives toward new capabilities in the field of autonomous tactical vehicles (ARCIC, 2014) (Tourner & Clow, 2016) that will become more depended on the commercial market (Fahey, 2015)it will become increasingly more difficult to ensure military standard of security will be developed within the commercial architectures. These factors increase the risks associated with the development of autonomous tactical vehicles.

References

Ackerman, E. (2015, March 23). *Tesla Model S: Summer Software Update Will Enable Autonomous Driving*. Retrieved August 6, 2015, from http://spectrum.ieee.org/: http://spectrum.ieee.org/cars-that-think/transportation/self-driving/tesla-model-s-to-combine-safety-sensors-to-go-autonomous

Aerospace Industries Association of America, Inc. (2011). *Defense Acquisition Reform: Moving Toward an Efficient Acquisition System.* Arlington: Aerospace Industries Association of America, Inc.

ARCIC. (2014, August 5). Training and Doctrine Command's (TRADOC) Technology and Capability Objectives for Force 2025 and Beyond. *INFORMATION PAPER*, 5. ARCIC. Retrieved August 5, 2015, from http://www.arcic.army.mil/app_Documents/ARCIC_InformationPaper_TRADOC-Technology-and-Capability-Objectives-for-Force-2025-and-Beyond_18AUG14.pdf

Army G8. (2010). *The Army Tactical Wheeled Vehicle Strategy.* Retrieved from Army G8: www.g8.army.mil/pdf/the_army_twv_strategy.pdf

Atkinson, D. J. (2015). *Emerging Cyber-Security Issues of Autonomy and the Psychopathology of Intelligent Machines.* Palo Alto, California: The AAAI Press. Retrieved August 5, 2015, from http://www.aaai.org/ocs/index.php/SSS/SSS15/paper/view/10219

Barkoviak, M. (2009, April 21). *Report:U.S. Fighter Project Infiltrated by CyberSpies*. Retrieved August 20, 2015, from IT, DailyTech: http://www.dailytech.com/Report+US+Fighter+Project+Infiltrated+by+Cyberspies/article14918.htm

Bartz, D. (2013, 11 05). U.S. Army AMAS: A Modular Approach to Truck Automation. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiz4JXYze3KAhVokYMKHQXlCCcQFggdMAA&url=http%3A%2F%2Forfe.princeton.edu%2F~alaink%2FSmartDrivingCars%2FITFVHA13%2FITFVHA13_US_DOD_AMAS_Bartz.pdf&usg=AFQjCNEWRdSYY6G3fR

Benjamin Braun, N. T. (2015). *Global Defense Outlook 2015 Defense and Development.* Deloitte. Retrieved from http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-2015-deloitte-global-defense-outlook.pdf

Boyd, C. J. (2008). *Globalized Military Industry: Are Army Program Managers Prepared to Manage the Risk?* Southfield: Lawrence Technological Univeristy.

Bryan, J., & Gulzelsu, O. (2014). *Inquiry Into Cyber Security Intrusions Affecting U.S. Transportation Company Contractors.* Senate, 113th Congress, 2nd Session. Washington: U.S. Governement Printing Office. Retrieved August 19, 2015, from http://www.armed-services.senate.gov/download/sasc_cyberreport_09-17-14

Carter, A. (2015). *THE DEPARTMENT OF DEFENSE CYBER STRATEGY.* Washington.

Chris Valasek, C. M. (2015). *Remote Exploitation of an Unaltered Passenger Vehicle.* IOACTIVE Hardware Software Wetware Security Services. Retrieved from http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf

CPS PWG Draft Framework for Cyber-Physical Systems, Release 0.8 1. (2015, September). Retrieved from www.cpspwg.org and http://www.nist.gov/cps/.:

http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf

Cyber Physical Systems. (2015, 6 3). Retrieved from https://www.nitrd.gov/: https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf

DAU . (n.d.). *Cybersecurity Training & Continuous Learning*. Retrieved from http://www.dau.mil/OtherProducts/pages/cybersecurity.aspx

DAU. (n.d.). *TRAINING STANDARDS & CORE PLUS DEVELOPMENT GUIDE INTERNATIONAL ACQUISITION*. Retrieved from DAU : http://icatalog.dau.mil/onlinecatalog/careerLvlInt.aspx?lvl=1&cfld=18

Dewey, C. (2013, May 28). *The U.S. weapons systems that experts say were hacked by the Chinese*. Retrieved August 20, 2015, from The Washington Post: https://www.washingtonpost.com/blogs/worldviews/wp/2013/05/28/the-u-s-weapons-systems-that-experts-say-were-hacked-by-the-chinese

DoD CIO 8500.01. (2014, March 14). Department of Defense INSTRUCTION Cybersecurity. *NUMBER 8500.01*. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwisp-XSib7KAhXIvYMKHRC-BFgQFggcMAA&url=http%3A%2F%2Fwww.dtic.mil%2Fwhs%2Fdirectives%2Fcorres%2Fpdf%2F850001_2014.pdf&usg=AFQjCNE7NC473xwOXXkldc74381XOTMrhw&bvm=b

DoD CIO 8510.01. (2014, March 12). Risk Management Framework (RMF) for DoD Information Technology (IT). *Department of Defense Instruction (DoDI) 8510.01*.

Eric Ke Wang, Y. Y. (2010). Security Issues and Challenges for Cyber Physical System. *IEEE* (pp. 733-738). 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference. Retrieved from http://people.cis.ksu.edu/~danielwang/Investigation/CPS_Security_threat/05724910.pdf

Fahey, K. (2015, July-August). *Integrating Innovation Keeping the Leading Edge.* Retrieved August 05, 2015, from Defense Aquisition, Technology and Logistics: http://dau.dodlive.mil/files/2015/06/DATL_Jul_Aug2015.pdf

Federal Procurement Data System - Next Generation. (2014). *Top 100 Contractor Report.* Retrieved from Federal Procurement Report: https://www.fpds.gov/downloads/top_requests/Top_100_Contractors_Report_Fiscal_Year_2014_v3.xls

Gary Silberg KPMG LLP, R. W. (n.d.). *www.kpmg.com.* Retrieved from https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-next-revolution.pdf

GENERAL DYNAMICS CORPORATION. (2014, December 31). GENERAL DYNAMICS CORPORATION. *NNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934(Commission File Number 1-3671).* Retrieved from http://www.sec.gov/Archives/edgar/data/40533/000004053315000009/gd-2014123110k.htm#s7B50484D46E2899F2183A9D70B9997A1

Google. (2015, July). *Google Self-Driving Car Project Monthly Report July 2015.* Google. Retrieved August 5, 2015, from http://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0715.pdf

Guay, T. R. (2007, February). GLOBALIZATION AND ITS IMPLICATIONS FOR THE DEFENSE INDUSTRIAL BASE. *Strategic Studies Institute*. doi:ISBN 1-58487-281-0

House of Representative 114TH CONGRESS. (2015). *NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2016.* WASHINGTON: U.S. GOVERNMENT PUBLISHING OFFICE.

International Monetary Fund. (1997). World Economic Outlook, May. *International Monetary Fund*, 45.

James Gosler, L. V. (2012). *DSB TASK FORCE REPORT Resilient Military Systems and the Advanced Cyber Threat.* DEFENSE SCIENCE BOARD | DEPARTMENT OF DEFENSE. Retrieved from http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

John Verrico, D. (2015, October 29). *DHS S&T Awards HRL Laboratories $2.5M for Automotive Cyber Security Research*. Retrieved from http://www.dhs.gov/science-and-technology/news/2015/10/29/st-awards-hrl-labs-25m-automotive-cyber-security-research

Kevin Dehoff, J. D. (2013, April). Managing a downturn: How the US defense industry can learn from its past. McKinsey & Company.

Lockheed Martin. (n.d.). LOCKHEED MARTIN CORPORATION 2014 ANNUAL REPORT. Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/2014-Annual-Report.pdf

Lyngaas, S. (2016, March 29). *Dunford: U.S. has work to do in cyber deterrence*. Retrieved from FCW The Business of Federal TEchnology: Cybersecurity: https://fcw.com/Articles/2016/03/29/dunford-cyber-lyngaas.aspx

Lyngaas, S. (2016, February 2). *Pentagon Chief: 2017 budget includes $7B for cyber*. Retrieved from The Business of Federal Technology: https://fcw.com/articles/2016/02/02/dod-budget-cyber.aspx

McCormack, R. A. (2015, May 20). U.S. Military Enters A New Era Defined By Globalization Of Its Technology Supply Chain. *Manufacturing and Technology News, Volume 22*(7). Retrieved from http://www.manufacturingnews.com/news/2015/New-Era-For-Defense-Industry-0520151.html

McNally, D. (2014, November 10). *Army focuses on autonomous system development*. Retrieved August 5, 2015, from U.S. Army, www.army.mil: http://www.army.mil/article/137718/Army_focuses_on_autonomous_system_development/

Mick, J. (2011, May 30). *Science*. Retrieved from Science, DailyTech: http://www.dailytech.com/Reports+Hackers+Use+Stolen+RSA+Information+to+Hack+Lockheed+Martin/article21757.htm

Miklaszewski, C. K. (2015, August 6). *CYBERSECURITY*. Retrieved August 19, 2015, from Russia hacks Pentagon computers: NBC, citing sources: http://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html

MORGAN, R. V. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, 607-610.

Nakashima, E. (2013, May 27). *Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-

weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

National Science Foundation. (n.d.). *Cyber-Physical Systems (CPS)*. Retrieved from Directorate for Computer & Information Science & Engineering: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286

NIST Directorate for Computer & Information Science & Engineering. (2016, February 4). *Cyber-Physical Systems (CPS)* . Retrieved from Directorate for Computer & Information Science & Engineering: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286

NORTHRUM GRUMMAN. (2015, March 18). 2014 Annual Report. Retrieved from http://www.northropgrumman.com/AboutUs/AnnualReports/Documents/pdfs/2014_noc_ar.pdf

Office of Personnel Management. (n.d.). *Cybersecurity Incidents*. Retrieved August 19, 2015, from Information about OPM Cybersecurity Incidents: https://www.opm.gov/cybersecurity/

Office of the Press Secretary. (2015, January 15). *SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts.* Retrieved August 19, 2015, from The White House Office of the Press Secretary: https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. (n.d.). *INTERNATIONAL COOPERATION IN DOD ACQUISITION*. Retrieved from Office of the Under Secretary of Defense for Acquisition, Technology and Logistics: http://www.acq.osd.mil/ic/CoopAcq.html

PLUNKETT, D. A. (2012, March 12). SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS. *CNSSI No. 1253*. Ft. Meade, Maryland: National Security Agency.

Ramey, J. (2015, May 15). *Autoweek*. Retrieved August 5, 2015, from http://autoweek.com/article/technology/freightliner-wants-know-if-were-ready-autonomous-trucks

RAYTHEON COMPANY. (2015, 2 11). RAYTHEON 10K SEC . *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES*.

Rosenzweig, D. I. (2014, October 27). *Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation*. Retrieved from The Heritage Foundation Issue Brief #4288: http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government

Rosenzweig, P. (2012, May 24). *The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government #2695*. Retrieved from The Heritage Foundation: http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government

SAE. (2016, March 31). *ybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Retrieved from Society of Automotive Engineers (SAE): http://standards.sae.org/wip/j3061/

Silberg, G. (n.d.). *Self-Driving Cars: Are We Ready?* Retrieved August 5, 2015, from www.KPMG.com: https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-are-we-ready.pdf

Snyder, B. (2014, October 3). *Cyber*. Retrieved August 19, 2015, from 5 huge cybersecurity breaches at companies you know: http://fortune.com/2014/10/03/5-huge-cybersecurity-breaches-at-big-companies/

Snyder, G. R. (2016, January 19). 2016 Michigan State of the State Transcript. Lansing, Michigan. Retrieved from http://www.michigan.gov/documents/snyder/2016_Michigan_State_of_the_State_Transcript_511676_7.pdf

Software Engineering Institue - Carnegie Mellon University. (n.d.). *Cyber-Physical Systems*. Retrieved from Software Engineering Institue - Carnegie Mellon University: http://www.sei.cmu.edu/cyber-physical/

TARDEC Public Affairs. (2014, December 16). *Leading Army researcher: Future of autonomous vehicles.* Retrieved August 5, 2015, from U.S. Army: http://www.army.mil/article/139889/Leading_Army_researcher__Future_of_autonomous_vehicles/

The White House;Office of the Press Secretary. (2015, February 13). *Foreign Policy*. Retrieved August 19, 2015, from FACT SHEET: White House Summit on Cybersecurity and Consumer Protection: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Theisen, B. (2011, February 14). Autonomous Mobility Appliqué System (AMAS). *SAE*, (p. 18). Retrieved August 5, 2015, from AMREL.com: http://www.sae.org/events/training/symposia/ivs/presentations/2011/bernard_theisen.pdf

Theisen, B. (2011, June 23). *Autonomous Mobility AppliquéSystem(AMAS) JCTD FY12-13 Industry Day.* US Army RDECOM-TARDEC. TARDEC .

Tourner, M. M., & Clow, M. M. (2016, February 23). *PEO CS&CSS works to sharpen the Army's teeth while trimming its tail*. Retrieved from Tooth to Tail: http://asc.army.mil/web/access-log-tooth-to-tail/

U.S. Department of Commerce Bureau of Industry and Security. (2015, March). "Offsets in Defense Trade Nineteenth Study".

U.S. Department of Transportation . (2014). *Characterization of Potential Security Threats in Modern Automobiles, A Composite Modeling Approach.* National Highway Traffic Safety Administration. Retrieved August 5, 2015, from http://ntl.bts.gov/lib/52000/52800/52887/Characterization_Potential_Threats_Autos-090314.pdf?utm_source=GovDelivery&utm_medium=email%20&utm_campaign=TRB%20October

UNITED TECHNOLOGIES CORP. (2015, 05 05). *2014 FORM 10-K* . Retrieved from http://files.shareholder.com/downloads/UTX/1387494618x0xS101829-15-5/101829/filing.pdf

USAASC. (n.d.). *USAASC Director*. Retrieved from USAASC: http://asc.army.mil/web/usaasc-director/

Wikipedia. (2016, March 31). *Likert scale*. Retrieved from wikipedia: https://en.wikipedia.org/wiki/Likert_scale

Glossary of Acronyms and Terms

AT&L.....Acquisition, Technology and Logistics

DAG.....Defense Acquisition Guidebook

DAU.....Defense Acquisition University

DCMA.....Defense Contract Management Agency

DoD.....Department of Defense

DoDD.....Department of Defense Directive

GAO .....Government Accountability Office

GPQ .....Group Process Questionnaire

H_0 .....Null Hypothesis

H_1 .....Alternate Hypothesis

IPPD .....Integrated Product and Process Development

IPT .....Integrated Product Team

USD(AT&L)..Under Secretary of Defense for Acquisition, Technology and Logistics

Appendix A – Survey

1. Hello!

My name is Sebastian Iovannitti (sebastian.c.iovannitti.civ@mail.mil) and I am currently enrolled as a graduate student in the Department of Management, Lawrence Technological University and as a Fellow in the Defense Acquisition University's (DAU's) Senior Service College Fellowship Program evaluating the effects Cyber Policies and Guidance on Acquisition programs.

As an adult 18 years of age or older, you agree to participate in this survey. You understand that your participation is entirely voluntary. You can withdraw your consent at any time. By agreeing to participate in this study, you indicate that you understand the following:

1: If you choose to participate, you will be asked to complete an online questionnaire. The questionnaire will include items relating to demographics and DoD Guidance and Policy on Cyber Security. The questionnaire will take approximately 15 to 20 minutes to complete.

2: There will be no incentive for participation.

3: All items in the questionnaire are important for analysis, and data will be more meaningful if all questions are answered. You can discontinue participation at any time without penalty by exiting out of the survey.

4: This research will not expose you to any discomfort or stress beyond that which might normally occur during a typical day. There are no right or wrong answers; thus, you need not be stressed about finding a correct answer.

5: Data collected will be handled in a confidential manner. The data collected will remain anonymous.

The purpose of this research has been explained and your participation is entirely voluntary. YOU MAY PRINT THIS PAGE FOR YOUR RECORDS.

Research at DAU that involves human participants is carried out under the oversight of an Institutional Review Board.

- ○ I have read this informed consent and I AGREE to participate
- ○ I have read this informed consent and I DO NOT AGREE to participate

"Globalized Contractor" is defined an entity that is utilizing globalization to its advantage. It may meet any of the following attributes:

Has a customer base outside the United States;
United States-based with operations distributed across the Globe;
Contracts software or hardware development or integration offshore;
Owns subsidiaries or other entities based outside the United States;
Routinely uses subcontractors that are either foreign-owned or based outside the United States;
Employs foreign nationals;
Owned or partially owned by a foreign government or foreign corporation.

2. What ACAT Level is your current program?

- ◯ ACAT IV
- ◯ ACAT III
- ◯ ACAT II
- ◯ ACAT I (any)
- ◯ Other (please specify)

3. Which one of the following statements below best characterizes your current program? (Choose ONE only).

- ◯ Hardware Intensive
- ◯ Software Intensive
- ◯ Mix of Hardware/Software
- ◯ Commercial Off The Shelf (COTS)
- ◯ Other (please specify)

4. Does your system have collaborating computational subsystems controlling physical entities ?

- ◯ Yes
- ◯ No

5. Which definition best describes your system:

- ◯ Platform Information Technology(PIT): IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.
- ◯ Cyber Physical System (CPS):Collaborating computational subsystems controlling physical entities
- ◯ Other (please specify)

6. Given the definition above for a globalized contractor, do you perceive your current contractors to be globalized contractors ?

- ◯ Yes
- ◯ No

7. Please indicate your level of agreement with the following statements when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. There is an increased cost and schedule risk due to EXPORT/IMPORT controls (ITAR, TAA Etc.)	◯	◯	◯	◯	◯
b. It increases complexity to TECHNICAL DATA PROTECTION	◯	◯	◯	◯	◯
c. COST & SCHEDULE impacts increased due to Cyber Security Guidance and Policies	◯	◯	◯	◯	◯
d. PROGRAM DISRUPTION AT FOREIGN SITES due to lack of cyber security measures	◯	◯	◯	◯	◯

8. Please indicate your level of agreement with the following statements when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. OBTAINING STATE OF THE ART TECHNOLOGY due to complexity of the export/import control process.	○	○	○	○	○
b. OBTAINING STATE OF THE ART TECHNOLOGY due to emphasis on producing the technology in the United States.	○	○	○	○	○
c. Cyber Security Policy/Guidance impacts negatively program costs .	○	○	○	○	○
d. Cyber Security Policy/Guidance impacts negatively program schedule.	○	○	○	○	○

9. Please indicate your level of agreement with the following statements when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. Increased cyber risks to SOFTWARE SECURITY/INTEGRITY due to offshore development	○	○	○	○	○
b. Increased cyber risks to SOFTWARE SECURITY/INTEGRITY from foreign nationals working at U.S. Defense Contractors	○	○	○	○	○
c. Increased cyber risks to SOFTWARE/SECURITY INTEGRITY from the use of COTS SW developed from offshore sources	○	○	○	○	○

10. Please indicate your level of agreement with the following statements.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a.Information is not disclosed to system entities unless they have been authorized to access the information	○	○	○	○	○
b.Systems/Subsystems have integrity to guard against improper information modification (includes ensuring information non-repudiation and authenticity)	○	○	○	○	○
c.Systems are available and ensure timely and reliably access to and use of information/date	○	○	○	○	○
d.Reciprocity agreements will be simple to develop	○	○	○	○	○

11. Within my program an Information System Security Manager (ISSM) is assigned to each system?

- ○ Yes
- ○ No
- ○ Unsure

12. Please indicate your level of agreement/disagreement that the Information System Security Manager (ISSM) has the;

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
SUPPORT to satisfy the responsibilities within the Risk Management Framework.	○	○	○	○	○
AUTHORITY to satisfy the responsibilities within the Risk Management Framework.	○	○	○	○	○
RESOURCES to satisfy the responsibilities within the Risk Management Framework.	○	○	○	○	○

13. Please indicate your level of agreement/disagreement that there is an increased cyber risk in the following areas when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. Increased cyber risk to COMPONENT/SUBSYSTEM MATERIAL AVAILABILITY when the globalized contractor uses foreign sources	○	○	○	○	○
b. Increased cyber risk to PRODUCTION of END ITEMS due to the use of OFFSHORE PRODUCERS (e.g. FAR/DFAR restrictions, Exotic Material Legislation	○	○	○	○	○
c. Increased cyber risk to INTEGRATION OF HARDWARE developed by both U.S. and foreign sources	○	○	○	○	○

14. Please indicate your level of agreement/disagreement that there is an increased cyber risk in the following when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. Increased cyber risk to SUPPLY CHAIN DISRUPTION	○	○	○	○	○
b. Increased cyber risk to OCONUS FIELDING due to the use of FOREIGN NATIONALS	○	○	○	○	○

15. Please indicate your level of agreement/disagreement that there is an increased cyber risk in the following areas when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. Increased cyber risk due to LANGUAGE DIFFERENCES (including understanding intent of scope)	○	○	○	○	○
b. Increased cyber risk due to POLITICAL ISSUES either internal to a foreign country or external with the United States	○	○	○	○	○
c. Increased cyber risk due to LEGAL DIFFERENCES in foreign countries (cyber laws, business laws)	○	○	○	○	○
d. Increased cyber risk due to CULTURAL DIFFERENCES and GLOBAL FLASH POINTS (including religion)	○	○	○	○	○
e. Increased cyber risk due to GEOGRAPHICAL DISPERSED/VIRTUAL WORKFORCE	○	○	○	○	○

LIFECYCLE are impacted by cyber risks when using a globalized contractor.

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
a. MATERIEL SOLUTION ANALYSIS	○	○	○	○	○
b. TECHNOLOGY MATURATION AND RISK REDUCTION	○	○	○	○	○
c. ENGINEERING AND MANUFACTURING DEVELOPMENT	○	○	○	○	○
d. PRODUCTION	○	○	○	○	○
e. FIELDING/DEPLOYMENT	○	○	○	○	○
f. DISPOSAL	○	○	○	○	○

17. POLICY/GUIDANCE was effective in preparing me to identify plan for cost and schedule due to CYBER risks?

- ○ Strongly Agree
- ○ Agree
- ○ Neither Agree or Disagree
- ○ Disagree
- ○ Strongly Disagree

18. POLICY/GUIDANCE was effective in preparing me to identify and plan for CYBER risks to TECHNICAL DATA PROTECTION?

- ○ Strongly Agree
- ○ Agree
- ○ Neither Agree or Disagree
- ○ Disagree
- ○ Strongly Disagree

19. POLICY/GUIDANCE was effective in preparing me to identify and plan for potential PROGRAM DISRUPTION AT FOREIGN SITES due to cyber security risks?

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

20. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk OBTAINING STATE OF THE ART TECHNOLOGY?

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

21. POLICY/GUIDANCE was effective in preparing me to identify and plan for cyber risk to SOFTWARE SECURITY/INTEGRITY due to offshore or use of foreign nationals.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

22. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to SOFTWARE SECURITY/INTEGRITY due to offshore or use of foreign nationals.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

23. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to SOFTWARE SECURITY/INTEGRITY from using COTS SW developed offshore.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

24. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to COMPONENTS from foreign sources.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

25. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to INTEGRATION OF HARDWARE developed by both U.S. and foreign sources (e.g. technical data delivery, quality control, interoperability).

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

26. POLICY/GUIDANCE was effective in preparing me to identify and plan for SUPPLY CHAIN DISRUPTION (e.g. Army not biggest customer, export/import control)

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

27. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to OCONUS FIELDING due to use of FOREIGN NATIONALS.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

28. POLICY/GUIDANCE was effective in preparing me to identify and plan for LANGUAGE DIFFERENCES (understanding of intent) .

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

29. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to POLITICAL ISSUES either internal to the foreign country or with the U.S.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

30. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to LEGAL DIFFERENCES in foreign countries.

- Strongly Agree
- Agree
- Neither Agree or Disagree
- Disagree
- Strongly Disagree

31. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to CULTURAL DIFFERENCES and GLOBAL FLASHPOINTS (e.g. religious ideology, holidays).

- ○ Strongly Agree
- ○ Agree
- ○ Neither Agree or Disagree
- ○ Disagree
- ○ Strongly Disagree

32. POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to the contractor using GEOGRAPHICALLY DISPERSED/VIRTUAL WORKFORCE.

- ○ Strongly Agree
- ○ Agree
- ○ Neither Agree or Disagree
- ○ Disagree
- ○ Strongly Disagree

33. Which of the following type of FORMAL PM training have you used? (CHECK ALL THAT APPLY)

- [ ] DAU Program Management Classes
- [ ] ICAF/National Defense University
- [ ] Other Senior Service Schools
- [ ] University/College Courses
- [ ] Defense Systems Management College
- [ ] Other (please specify)

34. Which of the following learning objectives and/or learning opportunities should be included in ANY formal training classes to address the risk posed when using a globalized contractor?

- [ ] Cyber Security
- [ ] Export/Import Regulations, Laws, and Processes
- [ ] International Business and Contracting Introduction
- [ ] Understanding what is Globalization
- [ ] Impacts of Globalization
- [ ] Causes of Globalization
- [ ] U.S. Production Policies Affecting DoD
- [ ] Utilizing industry globalization training
- [ ] Introduction to international law
- [ ] Global Economics
- [ ] Other (please specify)

35. How long have you been a Program Manager? (current and/or previous PM)

- ( ) 0-3 years
- ( ) 4-6 years
- ( ) 7-10 years
- ( ) 10+ years

36. What type of programs have you been a PM for?

- [ ] ACATIV
- [ ] ACAT III
- [ ] ACAT II
- [ ] ACAT I (any)
- [ ] Other (please specify)

37. Please check all of the following functions that you are level III certified in?

- [ ] Auditing
- [ ] Business, Cost Estimating and Financial Management
- [ ] Contracting
- [ ] Facilities Engineering
- [ ] Industrial/Contract Property Management
- [ ] Information Technology
- [ ] Production, Quality and Manufacturing
- [ ] Purchasing
- [ ] Program Management
- [ ] Engineering
- [ ] Test and Evaluation
- [ ] Life Cycle Logistics
- [ ] Other (please specify)

38. What is the highest education level you have attained?

- ○ Bachelor's Degree
- ○ Post Bachelor Work
- ○ Master's Degree
- ○ Post Masters Work
- ○ Multiple Master's Degrees
- ○ Doctorate Degree
- ○ Post Doctorate Work

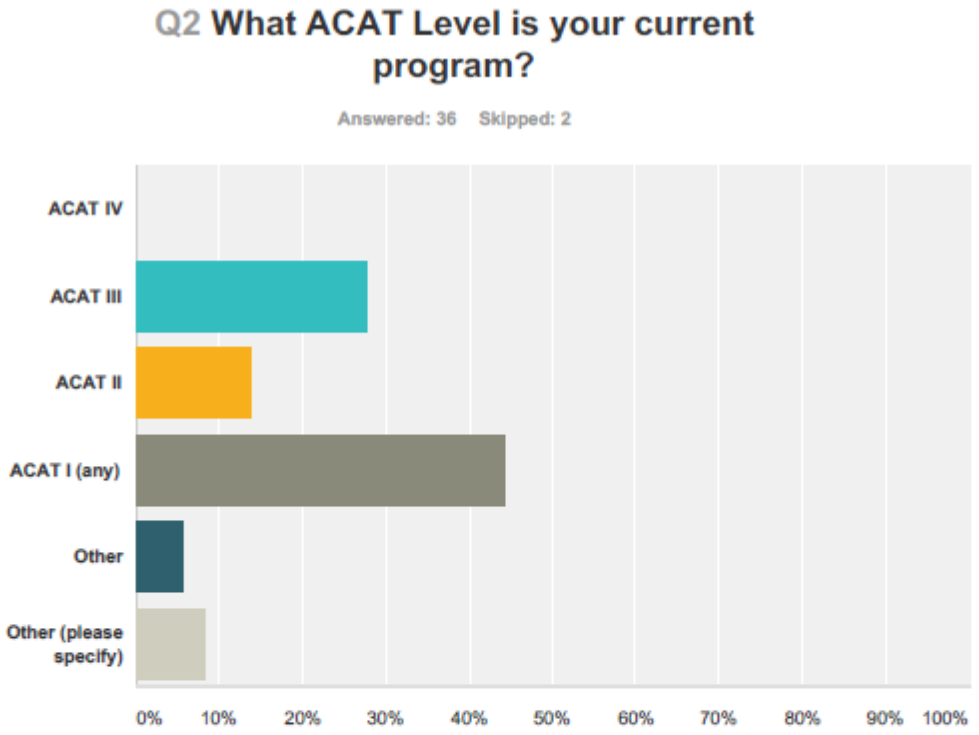
39. What risks you perceive there to be when using a GLOBALIZED CONTRACTOR?

40. What are the opportunities to attain RECIPROCITY with other PMs on Cyber Risks ?

41. What areas do you perceive need Cyber Security support?

42. Any additional Comments

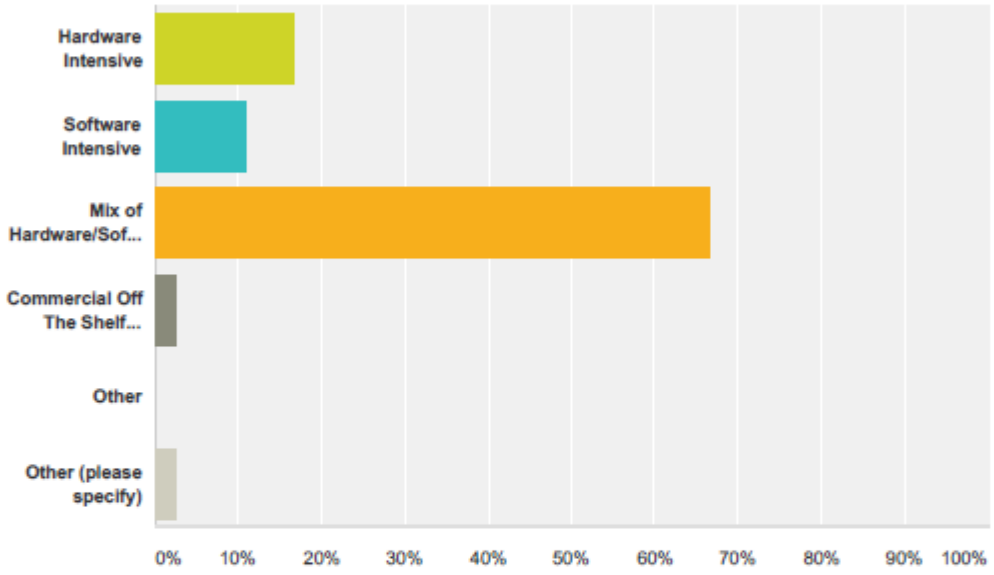
Appendix B- Survey Responses



Answer Choices	Responses	
ACAT IV	0.00%	0
ACAT III	27.78%	10
ACAT II	13.89%	5
ACAT I (any)	44.44%	16
Other	5.56%	2
Other (please specify)	8.33%	3
Total		36

Q3 Which one of the following statements below best characterizes your current program? (Choose ONE only).

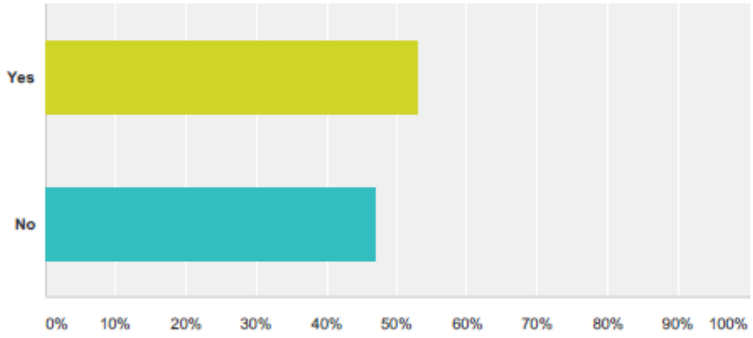
Answered: 36 Skipped: 2



Answer Choices	Responses	
Hardware Intensive	16.67%	6
Software Intensive	11.11%	4
Mix of Hardware/Software	66.67%	24
Commercial Off The Shelf (COTS)	2.78%	1
Other	0.00%	0
Other (please specify)	2.78%	1
Total		36

Q4 Does your system have collaborating computational subsystems controlling physical entities ?

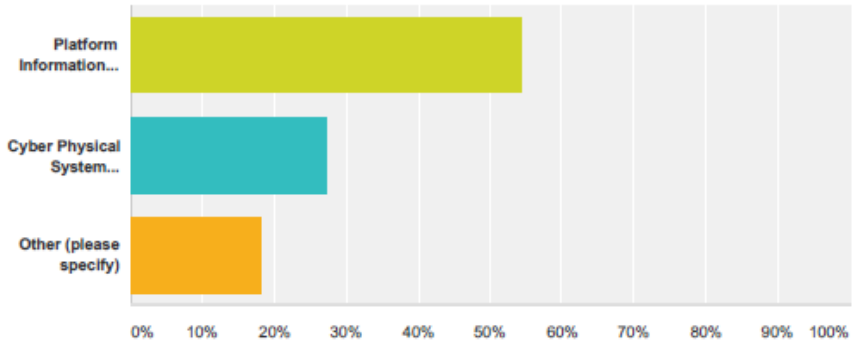
Answered: 34 Skipped: 4



Answer Choices	Responses	
Yes	52.94%	18
No	47.06%	16
Total		34

Q5 Which definition best describes your system:

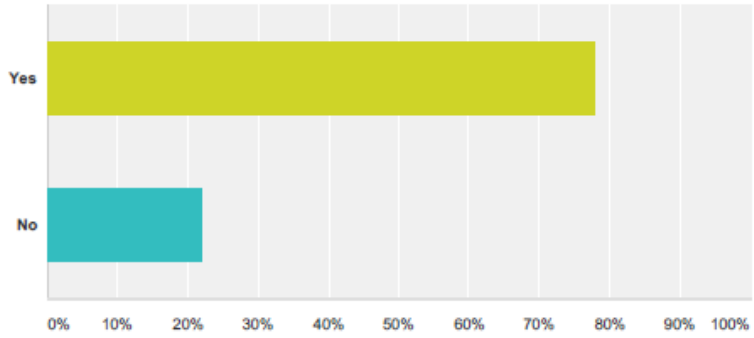
Answered: 11 Skipped: 27



Answer Choices	Responses
Platform Information Technology(PIT): IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.	54.55% 6
Cyber Physical System (CPS):Collaborating computational subsystems controlling physical entities	27.27% 3
Other (please specify)	18.18% 2
Total	11

Q6 Given the definition above for a globalized contractor, do you perceive your current contractors to be globalized contractors ?

Answered: 36 Skipped: 2



Answer Choices	Responses
Yes	77.78% 28
No	22.22% 8
Total	36

Q7 Please indicate your level of agreement with the following statements when using a globalized contractor.

Answered: 36 Skipped: 2

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. There is an increased cost and schedule risk due to EXPORT/IMPORT controls (ITAR, TAA Etc.)	22.22% 8	50.00% 18	16.67% 6	8.33% 3	2.78% 1	36
b. It increases complexity to TECHNICAL DATA PROTECTION	27.78% 10	55.56% 20	13.89% 5	0.00% 0	2.78% 1	36
c. COST & SCHEDULE impacts increased due to Cyber Security Guidance and Policies	27.78% 10	52.78% 19	11.11% 4	5.56% 2	2.78% 1	36
d. PROGRAM DISRUPTION AT FOREIGN SITES due to lack of cyber security measures	8.33% 3	27.78% 10	44.44% 16	13.89% 5	5.56% 2	36

Q8 Please indicate your level of agreement with the following statements when using a globalized contractor.

Answered: 36 Skipped: 2

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. OBTAINING STATE OF THE ART TECHNOLOGY due to complexity of the export/import control process.	11.11% 4	41.67% 15	30.56% 11	13.89% 5	2.78% 1	36
b. OBTAINING STATE OF THE ART TECHNOLOGY due to emphasis on producing the technology in the United States.	11.11% 4	47.22% 17	27.78% 10	11.11% 4	2.78% 1	36
c. Cyber Security Policy/Guidance impacts negatively program costs .	27.78% 10	52.78% 19	8.33% 3	11.11% 4	0.00% 0	36
d. Cyber Security Policy/Guidance impacts negatively program schedule.	19.44% 7	41.67% 15	27.78% 10	11.11% 4	0.00% 0	36

Q9 Please indicate your level of agreement with the following statements when using a globalized contractor.

Answered: 36 Skipped: 2

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. Increased cyber risks to SOFTWARE SECURITY/INTEGRITY due to offshore development	16.67% 6	50.00% 18	19.44% 7	13.89% 5	0.00% 0	36
b. Increased cyber risks to SOFTWARE SECURITY/INTEGRITY from foreign nationals working at U.S. Defense Contractors	8.33% 3	52.78% 19	30.56% 11	8.33% 3	0.00% 0	36
c. Increased cyber risks to SOFTWARE/SECURITY INTEGRITY from the use of COTS SW developed from offshore sources	22.22% 8	47.22% 17	25.00% 9	5.56% 2	0.00% 0	36

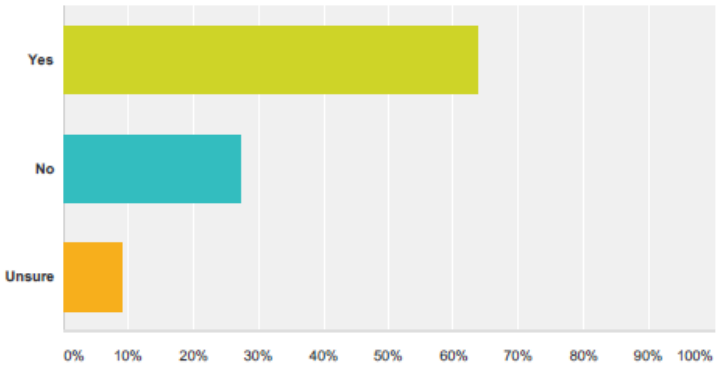
Q10 Please indicate your level of agreement with the following statements.

Answered: 36 Skipped: 2

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a.Information is not disclosed to system entities unless they have been authorized to access the information	25.00% 9	61.11% 22	11.11% 4	2.78% 1	0.00% 0	36
b.Systems/Subsystems have integrity to guard against improper information modification (includes ensuring information non-repudiation and authenticity)	11.11% 4	55.56% 20	33.33% 12	0.00% 0	0.00% 0	36
c.Systems are available and ensure timely and reliably access to and use of information/date	2.78% 1	66.67% 24	27.78% 10	2.78% 1	0.00% 0	36
d.Reciprocity agreements will be simple to develop	2.78% 1	13.89% 5	47.22% 17	30.56% 11	5.56% 2	36

Q11 Within my program an Information System Security Manager (ISSM) is assigned to each system?

Answered: 33 Skipped: 5



Answer Choices	Responses	
Yes	63.64%	21
No	27.27%	9
Unsure	9.09%	3
Total		33

Q12 Please indicate your level of agreement/disagreement that the Information System Security Manager (ISSM) has the;

Answered: 33 Skipped: 5

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
SUPPORT to satisfy the responsibilities within the Risk Management Framework.	24.24% 8	48.48% 16	15.15% 5	9.09% 3	3.03% 1	33
AUTHORITY to satisfy the responsibilities within the Risk Management Framework.	15.15% 5	54.55% 18	12.12% 4	15.15% 5	3.03% 1	33
RESOURCES to satisfy the responsibilities within the Risk Management Framework.	12.12% 4	33.33% 11	30.30% 10	21.21% 7	3.03% 1	33

Q13 Please indicate your level of agreement/disagreement that there is an increased cyber risk in the following areas when using a globalized contractor.

Answered: 33 Skipped: 5

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. Increased cyber risk to COMPONENT/SUBSYSTEM MATERIAL AVAILABILITY when the globalized contractor uses foreign sources	18.18% 6	66.67% 22	12.12% 4	3.03% 1	0.00% 0	33
b. Increased cyber risk to PRODUCTION of END ITEMS due to the use of OFFSHORE PRODUCERS (e.g. FAR/DFAR restrictions, Exotic Material Legislation	15.15% 5	57.58% 19	24.24% 8	3.03% 1	0.00% 0	33
c. Increased cyber risk to INTEGRATION OF HARDWARE developed by both U.S. and foreign sources	12.12% 4	63.64% 21	18.18% 6	6.06% 2	0.00% 0	33

Q14 Please indicate your level of agreement/disagreement that there is an increased cyber risk in the following when using a globalized contractor.

Answered: 33 Skipped: 5

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. Increased cyber risk to SUPPLY CHAIN DISRUPTION	21.21% 7	45.45% 15	24.24% 8	9.09% 3	0.00% 0	33
b. Increased cyber risk to OCONUS FIELDING due to the use of FOREIGN NATIONALS	9.09% 3	39.39% 13	33.33% 11	18.18% 6	0.00% 0	33

Q15 Please indicate your level of agreement/disagreement that there is an increased cyber risk in the following areas when using a globalized contractor.

Answered: 33 Skipped: 5

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. Increased cyber risk due to LANGUAGE DIFFERENCES (including understanding intent of scope)	6.06% 2	30.30% 10	39.39% 13	24.24% 8	0.00% 0	33
b. Increased cyber risk due to POLITICAL ISSUES either internal to a foreign country or external with the United States	15.15% 5	30.30% 10	48.48% 16	6.06% 2	0.00% 0	33
c. Increased cyber risk due to LEGAL DIFFERENCES in foreign countries (cyber laws, business laws)	18.18% 6	45.45% 15	33.33% 11	3.03% 1	0.00% 0	33
d. Increased cyber risk due to CULTURAL DIFFERENCES and GLOBAL FLASH POINTS (including religion)	15.63% 5	34.38% 11	40.63% 13	9.38% 3	0.00% 0	32
e. Increased cyber risk due to GEOGRAPHICAL DISPERSED/VIRTUAL WORKFORCE	16.13% 5	38.71% 12	29.03% 9	12.90% 4	3.23% 1	31

Q16 Pleases indicate your level of agreement/disagreement that the following phased of a PROGRAM'S LIFECYCLE are impacted by cyber risks when using a globalized contractor.

Answered: 33 Skipped: 5

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Total
a. MATERIEL SOLUTION ANALYSIS	9.38% 3	34.38% 11	21.88% 7	34.38% 11	0.00% 0	32
b. TECHNOLOGY MATURATION AND RISK REDUCTION	9.09% 3	60.61% 20	12.12% 4	18.18% 6	0.00% 0	33
c. ENGINEERING AND MANUFACTURING DEVELOPMENT	24.24% 8	66.67% 22	3.03% 1	6.06% 2	0.00% 0	33
d. PRODUCTION	24.24% 8	54.55% 18	12.12% 4	9.09% 3	0.00% 0	33
e. FIELDING/DEPLOYMENT	9.09% 3	45.45% 15	21.21% 7	24.24% 8	0.00% 0	33
f. DISPOSAL	6.06% 2	12.12% 4	24.24% 8	51.52% 17	6.06% 2	33

Q17 POLICY/GUIDANCE was effective in preparing me to identify plan for cost and schedule due to CYBER risks?

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	6.06%	2
Agree	12.12%	4
Neither Agree or Disagree	30.30%	10
Disagree	33.33%	11
Strongly Disagree	18.18%	6
Total		33

Q18 POLICY/GUIDANCE was effective in preparing me to identify and plan for CYBER risks to TECHNICAL DATA PROTECTION?

Answered: 32 Skipped: 6

Answer Choices	Responses	
Strongly Agree	6.25%	2
Agree	25.00%	8
Neither Agree or Disagree	37.50%	12
Disagree	21.88%	7
Strongly Disagree	9.38%	3
Total		32

Q19 POLICY/GUIDANCE was effective in preparing me to identify and plan for potential PROGRAM DISRUPTION AT FOREIGN SITES due to cyber security risks?

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	18.18%	6
Neither Agree or Disagree	42.42%	14
Disagree	24.24%	8
Strongly Disagree	12.12%	4
Total		33

Q20 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk OBTAINING STATE OF THE ART TECHNOLOGY?

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	27.27%	9
Neither Agree or Disagree	33.33%	11
Disagree	30.30%	10
Strongly Disagree	6.06%	2
Total		33

Q21 POLICY/GUIDANCE was effective in preparing me to identify and plan for cyber risk to SOFTWARE SECURITY/INTEGRITY due to offshore or use of foreign nationals.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	27.27%	9
Neither Agree or Disagree	36.36%	12
Disagree	27.27%	9
Strongly Disagree	6.06%	2
Total		33

Q22 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to SOFTWARE SECURITY/INTEGRITY due to offshore or use of foreign nationals.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	6.06%	2
Agree	24.24%	8
Neither Agree or Disagree	42.42%	14
Disagree	24.24%	8
Strongly Disagree	3.03%	1
Total		33

Q23 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to SOFTWARE SECURITY/INTEGRITY from using COTS SW developed offshore.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	12.12%	4
Neither Agree or Disagree	48.48%	16
Disagree	33.33%	11
Strongly Disagree	3.03%	1
Total		33

Q24 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to COMPONENTS from foreign sources.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	39.39%	13
Neither Agree or Disagree	39.39%	13
Disagree	15.15%	5
Strongly Disagree	3.03%	1
Total		33

Q25 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to INTEGRATION OF HARDWARE developed by both U.S. and foreign sources (e.g. technical data delivery, quality control, interoperability).

Answered: 32 Skipped: 6

Answer Choices	Responses	
Strongly Agree	6.25%	2
Agree	15.63%	5
Neither Agree or Disagree	53.13%	17
Disagree	18.75%	6
Strongly Disagree	6.25%	2
Total		32

Q26 POLICY/GUIDANCE was effective in preparing me to identify and plan for SUPPLY CHAIN DISRUPTION (e.g. Army not biggest customer, export/import control)

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	24.24%	8
Neither Agree or Disagree	39.39%	13
Disagree	27.27%	9
Strongly Disagree	6.06%	2
Total		33

Q27 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk to OCONUS FIELDING due to use of FOREIGN NATIONALS.

Answered: 32 Skipped: 6

Answer Choices	Responses	
Strongly Agree	3.13%	1
Agree	9.38%	3
Neither Agree or Disagree	62.50%	20
Disagree	18.75%	6
Strongly Disagree	6.25%	2
Total		32

Q28 POLICY/GUIDANCE was effective in preparing me to identify and plan for LANGUAGE DIFFERENCES (understanding of intent) .

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	0.00%	0
Agree	6.06%	2
Neither Agree or Disagree	69.70%	23
Disagree	18.18%	6
Strongly Disagree	6.06%	2
Total		33

Q29 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to POLITICAL ISSUES either internal to the foreign country or with the U.S.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	0.00%	0
Agree	3.03%	1
Neither Agree or Disagree	69.70%	23
Disagree	21.21%	7
Strongly Disagree	6.06%	2
Total		33

Q30 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to LEGAL DIFFERENCES in foreign countries.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	6.06%	2
Neither Agree or Disagree	54.55%	18
Disagree	30.30%	10
Strongly Disagree	6.06%	2
Total		33

Q31 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to CULTURAL DIFFERENCES and GLOBAL FLASHPOINTS (e.g. religious ideology, holidays).

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	3.03%	1
Agree	6.06%	2
Neither Agree or Disagree	60.61%	20
Disagree	24.24%	8
Strongly Disagree	6.06%	2
Total		33

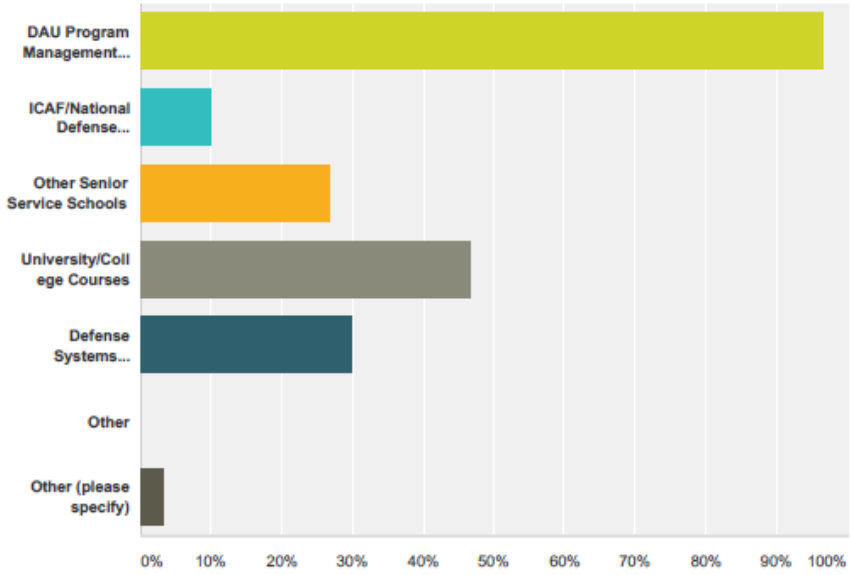
Q32 POLICY/GUIDANCE was effective in preparing me to identify and plan for increased cyber risk due to the contractor using GEOGRAPHICALLY DISPERSED/VIRTUAL WORKFORCE.

Answered: 33 Skipped: 5

Answer Choices	Responses	
Strongly Agree	0.00%	0
Agree	18.18%	6
Neither Agree or Disagree	54.55%	18
Disagree	24.24%	8
Strongly Disagree	3.03%	1
Total		33

Q33 Which of the following type of FORMAL PM training have you used? (CHECK ALL THAT APPLY)

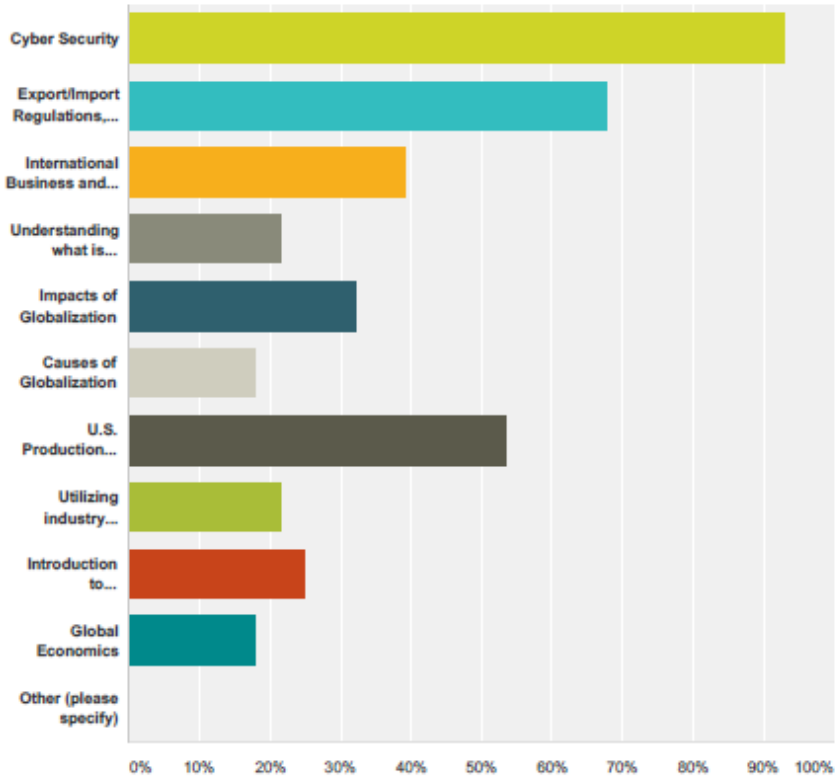
Answered: 30 Skipped: 8



Answer Choices	Responses	
DAU Program Management Classes	96.67%	29
ICAF/National Defense University	10.00%	3
Other Senior Service Schools	26.67%	8
University/College Courses	46.67%	14
Defense Systems Management College	30.00%	9
Other	0.00%	0
Other (please specify)	3.33%	1
Total Respondents: 30		

Q34 Which of the following learning objectives and/or learning opportunities should be included in ANY formal training classes to address the risk posed when using a globalized contractor?

Answered: 28 Skipped: 10

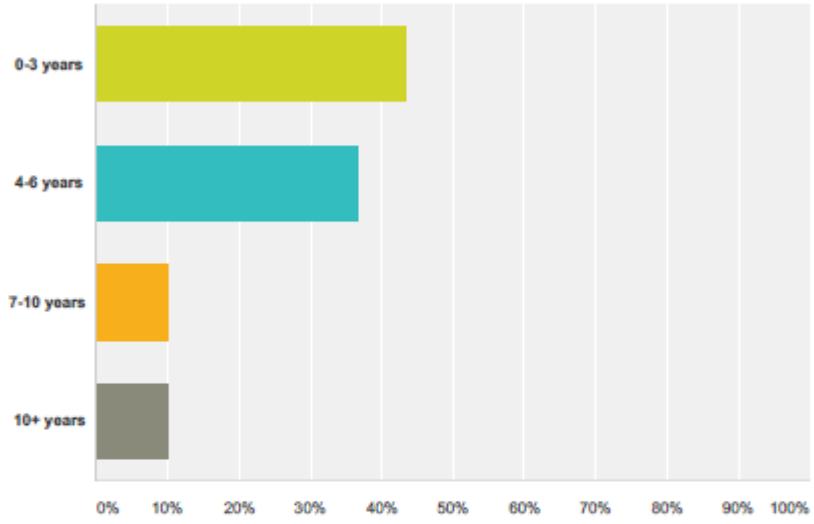


Answer Choices	Responses	
Cyber Security	92.86%	26
Export/Import Regulations, Laws, and Processes	67.86%	19
International Business and Contracting Introduction	39.29%	11
Understanding what is Globalization	21.43%	6
Impacts of Globalization	32.14%	9
Causes of Globalization	17.86%	5
U.S. Production Policies Affecting DoD	53.57%	15
Utilizing industry globalization training	21.43%	6

Introduction to international law	25.00%	7
Global Economics	17.86%	5
Other (please specify)	0.00%	0
Total Respondents: 28		

Q35 How long have you been a Program Manager? (current and/or previous PM)

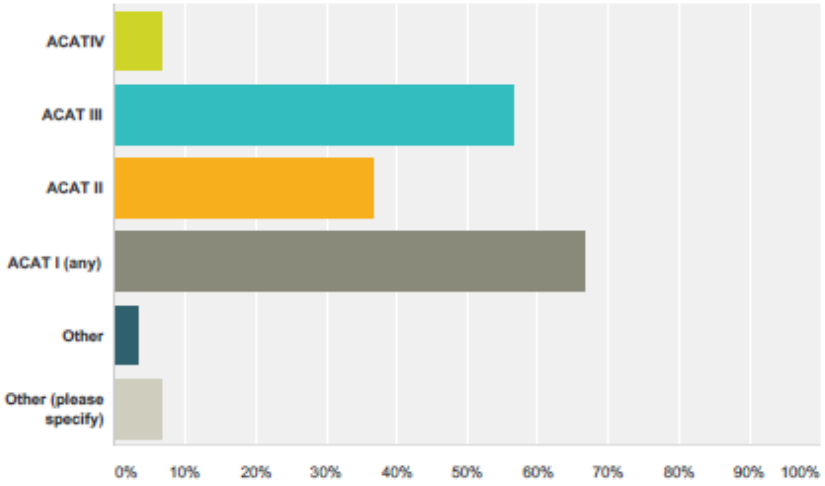
Answered: 30 Skipped: 8



Answer Choices	Responses	
0-3 years	43.33%	13
4-6 years	36.67%	11
7-10 years	10.00%	3
10+ years	10.00%	3
Total		30

Q36 What type of programs have you been a PM for?

Answered: 30 Skipped: 8



Answer Choices	Responses	
ACATIV	6.67%	2
ACAT III	56.67%	17
ACAT II	36.67%	11
ACAT I (any)	66.67%	20
Other	3.33%	1
Other (please specify)	6.67%	2
Total Respondents: 30		

Q37 Please check all of the following functions that you are level III certified in?

Answered: 30 Skipped: 8

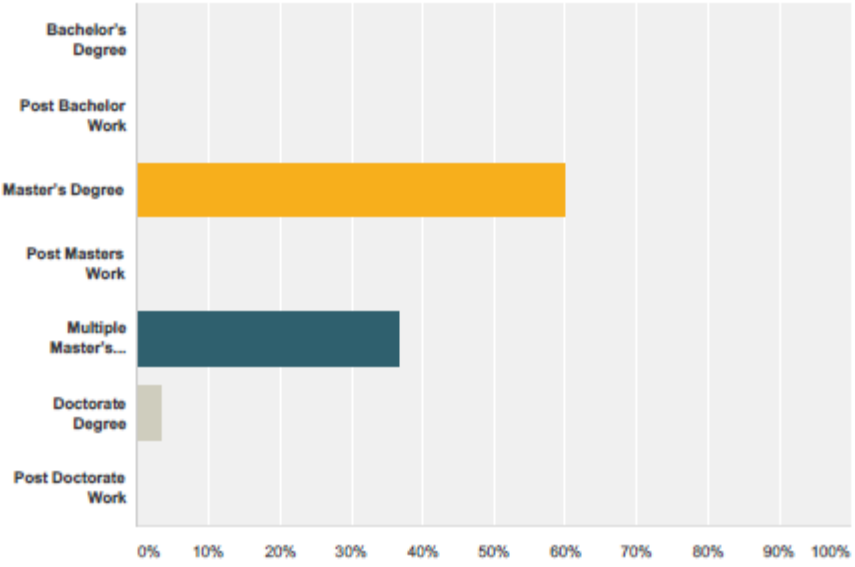
Answer Choices	Responses	
Auditing	0.00%	0
Business, Cost Estimating and Financial Management	3.33%	1
Contracting	10.00%	3
Facilities Engineering	0.00%	0
Industrial/Contract Property Management	0.00%	0

Cyber - ASAALT

Information Technology	3.33%	1
Production, Quality and Manufacturing	0.00%	0
Purchasing	0.00%	0
Program Management	100.00%	30
Engineering	3.33%	1
Test and Evaluation	3.33%	1
Life Cycle Logistics	3.33%	1
Other	0.00%	0
Other (please specify)	0.00%	0
Total Respondents: 30		

Q38 What is the highest education level you have attained?

Answered: 30 Skipped: 8



Answer Choices	Responses	
Bachelor's Degree	0.00%	0
Post Bachelor Work	0.00%	0
Master's Degree	60.00%	18
Post Masters Work	0.00%	0
Multiple Master's Degrees	36.67%	11
Doctorate Degree	3.33%	1
Post Doctorate Work	0.00%	0
Total		30

Q39 What risks you perceive there to be when using a GLOBALIZED CONTRACTOR?

Answered: 16 Skipped: 22

#	Responses	Date
1	firewalling	12/15/2015 2:34 PM
2	Awareness of additional industry risks	12/14/2015 4:24 PM
3	- technology exploitation	12/1/2015 3:44 PM
4	Definition is very broad. Any major contractor has a large international customer base, but not necessarily development, engineering, and manufacturing globally. Key is positive control and access of data.	12/1/2015 12:19 PM
5	na...don't use.	12/1/2015 11:51 AM
6	Inadverdant exposure to program specific information to other entities in a company.	11/30/2015 10:14 AM
7	Lack of understanding of evolving laws and policy with regards to cyber security.	11/30/2015 9:03 AM
8	1) Information exchange/Integrity 2) Cyber Security protocol 3) US Standards implementation	11/30/2015 8:57 AM
9	As long as the contract is well written with clear data rights, risk can be minimized	11/30/2015 7:38 AM
10	Slowed contracting and miscommunication	11/29/2015 11:01 PM
11	There will always be a level of risk to consider when a PM develops the acquisition plan. I have no issue using a Globalized Contractor to support my programs. We need laws and flexible regulations to ensure our US Industrial base is not hampered by more regulations, laws and oversight. Our globalized contractors must be able to compete within the US and globally to remain viable. With decreased defense spending, we need more flexibility and less regulations and oversight.	11/29/2015 1:02 PM
12	Theft of classified or sensitive data and technical specifications.	11/27/2015 7:22 AM
13	Protecting system vulnerabilities, hardware, software.	11/26/2015 7:58 PM
14	Supply chains for complex systems are long. Individual chips or other components can come from subcontractors that are 4-6 or more levels down from the prime vendor. Having full visibility and control of that supply chain is potentially impossible, creating opportunities for inserting something malicious in firmware, hardware, etc.	11/26/2015 9:00 AM
15	Globalized contractors can firewall programs so there is no connection to their non-US entities. For my program the contractor has done this.	11/25/2015 3:19 PM
16	Compromise of information, restricted information due to other nation's laws, different national allegnces.	11/25/2015 2:41 PM

Q40 What are the opportunities to attain RECIPROCITY with other PMs on Cyber Risks ?

Answered: 13 Skipped: 25

#	Responses	Date
1	none	12/15/2015 2:34 PM
2	- mitigate risks to exploitation and cost sharing opportunities	12/1/2015 3:44 PM
3	unknown	12/1/2015 12:19 PM
4	Continuous engagement.	11/30/2015 9:03 AM
5	1) Social Site 2) DAU share site 3) Acqui-pedia 4) Organizational level OPDs 5) Lessons learned portal	11/30/2015 8:57 AM
6	No sure what reciprocity means in this instance	11/30/2015 7:38 AM
7	Work toward a common standard	11/29/2015 11:01 PM
8	The opportunities exist. I am not sure how often it is used.	11/29/2015 1:02 PM
9	None	11/27/2015 7:22 AM
10	unknown	11/26/2015 7:58 PM
11	Uncertain what you mean by this question.	11/26/2015 9:00 AM
12	Won't happen unless OSD takes a greater leadership role.	11/25/2015 3:19 PM
13	Sharing of test information	11/25/2015 2:41 PM

Q41 What areas do you perceive need Cyber Security support?

Answered: 15 Skipped: 23

#	Responses	Date
1	none	12/15/2015 2:34 PM
2	Any program that has SW and touches a network	12/14/2015 4:24 PM
3	- funding for PoRs that fielded pre- Cyber Security emphasis	12/1/2015 3:44 PM
4	Protection of vehicle and airborne software and hardware from wireless access.	12/1/2015 12:19 PM
5	POM funding. cyber security is not developed into POM processes and POM does NOT support updates in cyber security requirements emerging	12/1/2015 11:26 AM
6	In each of the major functional areas listed above.	11/30/2015 9:03 AM
7	Any area pertaining to the development of equipment that exchanges/shares information across the DoDIN	11/30/2015 8:57 AM
8	We need ASA(ALT) to provide pre written CLINS for each level of Cyber Security - current system requires each of us to be an SME - need a centrol authroity	11/30/2015 7:38 AM
9	Any systems with a Net Ready KPP	11/29/2015 11:01 PM
10	Flexible laws and regulations. I, again, emphasize "flexible".	11/29/2015 1:02 PM
11	Sharing of contractor information on production status, failure investigation and test data	11/27/2015 7:22 AM
12	contracting policies on cyber security requirements, communicating the policy requirements to vendors.	11/26/2015 7:58 PM
13	You asked a large number of questions on my view of cyber security policy--I have to admit I have read none of it. In my office of 244 personnel, I have 2 people I consider experts, and another 5-6 that have a good understanding of Cyber. The rest of us know next to nothing. It may be beneficial for DAU to develop some course material that provides a general understanding for the majority of PMs, engineers, and logisiticians--rather than the tendency to just focus on better training the narrow stovepipe of individuals who focus on it (though we need that too).	11/26/2015 9:00 AM
14	The big defense contractors have implemented cyber defense measures. Their suppliers have not. That is the weak point of cyber defense.	11/25/2015 3:19 PM
15	Need to understand what is cyber testing RFM provieds some but it is constantly evolving with the necessary budget for PMs to support. Additional testing identified as necessary should be centrally funded or come at the expense of other testing.	11/25/2015 2:41 PM

Q42 Any additional Comments

Answered: 8 Skipped: 30

#	Responses	Date
1	A real, if not fully understood risk. As with any risk, avoid, mitigate, or transfer. No way for a PM to effectively transfer the risk except to the end-user but not an acceptable COA. Mitigation requires significant resourcing of dollars and expertise. Avoid through constraining vendor base, not exporting the product, other - though will not effectively protect/secure the product from vulnerabilities in the end.	12/1/2015 12:19 PM
2	Cyber Security is extremely important. No one is disputing...it is the cost that the PM is not resources for that is killing us....	12/1/2015 11:51 AM
3	Cyber Security has to be introduced at all Centers of Excellence (COE) because of the increased employment of net-centric communications based technology, whereas almost every Soldier has to operate	11/30/2015 8:57 AM
4	Questions 4, 5 & 39 would have been more insightful if you had included a definition	11/30/2015 7:38 AM
5	None	11/29/2015 11:01 PM
6	Cyber Security is one of many aspects a PM must consider when executing a program. We operate with multiple risk factors in mind.	11/29/2015 1:02 PM
7	*NSA process to approve architectures is something of a black box. There is no rule book you can follow and know with confidence that you will get approval. This creates a lot of risk--you have to design your architecture, slide it under the secret door and it comes back approved or not. If disapproved, you have unplanned redesign with associated cost and schedule impacts. I recognize that a "rule book" would be a double-edged sword--more certainty for material developers, but also a potential roadmap for adversaries. *I have not paid much attention to the fact that my prime is a global corporation. I have an approved Program Protection Plan for my 3 programs (2 ACAT ICs, and 1 pre-MDAP that will be an ACAT I if it gets approved to go forward), but operate under the assumption that other agencies within the USG are working to ensure that ITAR is met, security firewalls are in place to protect sensitive data, and the integrity of the supply chain is being monitored. Too many more immediate alligators at my level, so I expect I will never get to the point where I can put any time towards this area.	11/26/2015 9:00 AM
8	The Risk Management Framework was intended to allow PMs to find affordable solutions. Lately solutions are being prescribed - they were not planned for, budgeted, or scheduled - and often invalidate work accomplished on other solutions that had been implemented.	11/25/2015 3:19 PM

Appendix C – IRB Approval Letter

Institutional Review Board
Office of the Provost
research.ltu.edu irb@ltu.edu

October 26, 2015

Sebastian Iovannitti
Lawrence Technological University
College of Management
Senior Service College Fellowship Program
seba1865@gmail.com

Dear Mr. Iovannitti,

I am pleased to report that the IRB application to conduct research with human participants for your SSCF thesis "Cyber Security Considerations for Autonomous Tactical Wheeled Vehicles" has been approved under the Expedited review path for a period of one year, October 26, 2015 – October 26, 2016.

The IRB is satisfied that the following ethical concerns regarding the treatment of your human participants have been addressed in your research protocol: (1) The research involves administering a web-based survey to an individual who is at least 18 years of age or older in order to investigate if Cyber Security Policies have impacted project managers and how cyber security requirements could be identified for ground autonomous vehicles.; (2) Participants who will voluntarily consent to complete the survey are free to withdraw from the study at any time; (3) You have identified potential risks to you and the participants; and (4) You have assured that a balance exists between potential benefits of the research to the participants and/or society and the risk assumed by the participants.

Please contact the IRB if you require an extension to your project after one year. Please note you must contact the IRB if you make a change to your research protocol that impacts the ethical treatment of your research participants. Please do not hesitate to contact the IRB if you have any questions.

Sincerely,

Matthew Cole, Ph.D.
Chair, Institutional Review Board (IRB)
Lawrence Technological University
irb@ltu.edu o: 248.204.3096 f: 248.204.3099

Appendix D Certificate of Completion – Protecting Human Subject Research Participants

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **sebastian iovannitti** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 09/30/2015

Certification Number: 1877360

Author Biography

Sebastian Iovannitti is the Chief Systems Analysis for APEO SE&TI for PEO CS&CSS, developing the processes, infrastructure and policies deploying an enterprise knowledge, data and configuration management systems, enabling Acquisition aligning with PEO and Army Strategies (BPP, Force 2025). Before assuming his current duties, Mr. Iovannitti served as Deputy and Chief Systems Engineering for Product Directorate Contingency Basing leading the teams to develop a Model Base Systems Engineering construct supporting Contingency Base Camp Analysis, portfolios and Army Policy. Previously he was the, Assistant Program Executive Officer for Systems Engineering and Technology Integration (APEO SE&TI) Acting and the Lean Six Sigma (LSS) Deployment Director in the Program Executive Office for Combat Support and Combat Service Support (PEO CS&CSS), Warren, Michigan. While serving as Acting APEO SE&TI, Mr. Iovannitti has supported various high profile projects such as the PEO's fleet management, Vehicular Integration for C4ISR/EW Interoperability (VICTORY), Common Operating Environment (COE), LSS deployment, value engineering, continuous process improvement, and contingency basing initiatives. Previously he was the Senior Systems Engineer within the Army's Tank Automotive Research, Development and Engineering Center (TARDEC) and as a Senior Engineering Specialist within PEO CS&CSS supporting the Mine Resistant Ambush Protected (MRAP) program. Prior to entering civil service in 2007, Sebastian was a Senior Software/Systems Engineer at General Dynamics Land Systems (GDLS) supporting the Army's Future Combat Systems Manned Ground Vehicles, and a Systems Analyst at the Computer Science Corporation. He earned a MS in Engineering Management from the University of Michigan, and both a MS in Embedded Systems and a BS in Computer Science from Oakland University.

Mr. Iovannitti is a Certified Acquisition Professional Engineering and Program Management Level 3, an International Council on Systems Engineering (INCOSE) Certified Systems Engineering Professional (CSEP) -Acq, an American Society for Quality Certified Six Sigma Black Belt (BB), Army BB Certified, is a Department of Defense Army Acquisition Corps Member, and eCyberMission Virtual Judge. In 2010, Mr. Iovannitti was awarded the Army's LSS Excellence Award Program for the Enterprise Level Master BB Project, MRAP Requirements Management Program.